PERIODICAL FOR THE PROOFPOINT CUSTOMER COMMUNITY

ISSUE 5 / AUTUMN 2022

NEW PERIMETERS

PROTECT PEOPLE. DEFEND DATA.

Reinvent information security by prioritizing its two most critical components

proofpoint.

CONTENTS

ISSUE 5 / AUTUMN 2022

Magazine contributors

Ashan Willy
Chief Executive Officer, Proofpoint

Ryan Kalember
EVP, Cybersecurity Strategy, Proofpoint

Vincent Merlin
SVP, Global Marketing, Proofpoint

Sherrod DeGrippo
Vice President of Threat Research and Detection

Tim Choi
VP, Product Marketing, Proofpoint

Lucia Milică
VP and Global Resident CISO, Proofpoint

Adenike Cosgrove
VP, Marketing EMEA, Proofpoint

Jeremy Wittkop
Senior Director, Technology Services, Proofpoint

Matt Cooke
Director, Product Marketing, Proofpoint

Dr. BJ Fogg
PhD, Behavior Scientist at Stanford University

Ed Sleiman
Head of Information Security, King Abdullah University of Science and Technology (KAUST)

Sephanie Torto
Senior Product Marketing Manager, Proofpoint

Sai Chavali
Senior Product Marketing Manager, Proofpoint

Dave Cook
Senior Product Marketing Manager, Proofpoint

Sara Pan
Product Marketing Manager, Proofpoint

Mike Bailey
Product Marketing Manager, Proofpoint

Andrew Rose
Resident CISO, EMEA, Proofpoint

Sophie Ree
Content Marketing Manager, EMEA, Proofpoint

Welcome

WELCOME TO ISSUE 5 OF NEW PERIMETERS – PROTECT PEOPLE. DEFEND DATA.

There are no absolutes in cybersecurity. With threats constantly evolving and attackers adopting new strategies, one-dimensional approaches to security simply will not work, especially with threats like business email compromise, phishing and ransomware targeting your organization. That's why it's a priority to protect your two biggest assets: your people and your data. It is important to understand threat actors and how they attack your data, but also to analyze human behaviors that lead to breaches in the first place. It's time to get back to the basics of information security and do it the right way.

The path to protecting information goes through people

Of course, you must have visibility of your information but, most importantly, you need to understand what your employees are doing with it. The more insight you have, the better you can put protections in place for your people, and defend the data they have access to, share and use.

Information security is less about technology infrastructure and more about what it means to protect your information. People have access to information, and they get compromised. Now that 'work from anywhere' is a reality, this is more important than ever. Among the organizational chaos of remote and hybrid working, with people accessing data in many different ways that could harm your brand, protecting initial threat vectors such as email is vital.

In this issue, we explore the idea of reinventing information security by prioritizing its two most critical components: people and data. Ensuring your people have the knowledge, skills, and tools to safeguard your valuable intellectual property and assets. Protect people. Defend data.

Find out more

If you'd like to find out more about any of the topics you read in this issue, please get in touch with your Account Manager, or use our online form to contact us.

Contact us
proofpoint.com/us/contact

ASHAN WILLY
Chief Executive Officer,
Proofpoint

SECURING THE HOUSE

RYAN KALEMBER
EVP, Cybersecurity Strategy, Proofpoint

How to put protections where they matter most

As more of our data and networks make way to the cloud, organizations are now living in the same house.

From Proofpoint to Accenture. The Bank of England to a small high street café. We have the same front and back doors. The same lock mechanism. The same windows. The same perimeter fence - the same cloud productivity suites.

And we all store our valuables in these houses, behind these protections. To keep them safe from adversaries wishing to break in and take what's ours.

Secure the doors – and the people behind them

With limited budget and resources, encasing our house - Microsoft 365 and other cloud productivity applications - in impenetrable iron is not an option. Instead, we must place protections where they are needed most.

With over 90% of successful cyberattacks requiring human interaction, it is our people who need most protection. That's why any security solution starts with categorizing your VAPs (Very Attacked People) and targeting adaptive controls accordingly.

But single-point deterrents and defences alone are not enough. We need intelligent, multi-layered, people-centric security.

Business email compromise and supplier risk exceed all cybersecurity losses combined

99% of data loss incidents are people-centric

The vast majority of ransomware attacks start with email

Protect your house with Proofpoint

#1 for efficacy | #1 for the F500 | #1 for the Global 2000

Proofpoint – your integrated, consolidated platform for all attacks targeted at people

PRE-ATTACK: Build comprehensive security awareness with ongoing training in the modes and methods of modern cyber attacks:

- Phishing lures
- Compromised suppliers
- Spoofed domains
- Hijacked cloud accounts

MID-ATTACK: Implement additional layers of protection to stop threat actors in their tracks:

- Email threat protection
- Malware, phishing and BEC detection
- Warning flags
- Integration with EDR, IDP, and SIEM

POST-ATTACK: Initiate response and recovery to reduce disruption and better prepare for the next intruder.

- Automate containment of post-delivery detected threats
- Get visibility into your riskiest users and VAPs to retarget adaptive controls
- Analyze the attack chain with integrated dashboards and intelligent insight

Blurred lines.

Defending against data loss and cyber extortion with a holistic approach

WHY RANSOMWARE, BUSINESS EMAIL COMPROMISE (BEC), AND DATA LOSS HAVE MORE IN COMMON THAN YOU MIGHT THINK

It's safe to say that ransomware progressed beyond its epidemic stage and has now become endemic. It's having more of an impact on everyday lives than ever before, and no organization is immune. Proofpoint's 2022 State of the Phish report found that 68% of global organizations dealt with at least one ransomware infection stemming from a direct email payload, second-stage malware delivery, or other type of compromise. If you use the internet, you're a potential victim.

And just as the net of potential victims has widened, so too have the threat actors' business models.

Double and even triple extortion techniques are now prevalent. Exfiltrating large quantities of sensitive data and maintaining persistent access provide the opportunity to increase both the cost and type of their demands. Many ransomware groups, wary of attribution and the associated criminal indictments, have abandoned locker malware altogether and are simply stealing massive quantities of data and offering prices for both its sale and its destruction (buyer beware of the latter, especially).

RYAN KALEMBER
EVP, Cybersecurity Strategy, Proofpoint

Threat actors might evolve their business models, but their goal remains the same; to abuse access to your environment. The move away from locker malware to data theft is still extortion, and BEC actors moving from payroll and tax fraud to B2B cyber-enabled financial fraud is still BEC. Even more notably, a BEC actor looking for an unpaid invoice and a ransomware (or perhaps we should say "cyber extortion") group trying to steal data are going to rely on many of the same techniques, regardless of their monetization strategy.

These tools and techniques have been similar for years – compromising credentials, impersonation, user-activated malware, data theft, and so on. Regardless of where the threat landscape goes next, it's clear that viewing the main risk categories of ransomware, data extortion, BEC, and data loss as separate risk categories isn't optimal. Put another way, the advantage defenders have is that making those tools and techniques tougher for an adversary to use can make things equally difficult for multiple types of adversaries.

Meet the new foe, same as the old foe

Ransomware as data theft

Virtually 100% of ransomware incidents involve data theft, making it the most dominant form of extortion. In fact, many ransomware groups now focus solely on data theft and do not encrypt or try to destroy any information.

This makes for an incredibly problematic attack method. With data already outside your defenses, there is no guarantee that you'll get it back. Even if you do, it may already have been sold, exposed or leveraged against your organization in some other way – increasing the headache over whether to pay or not to pay.

Increasingly, organizations are opting not to pay, but this comes with obvious drawbacks. Most notably, fewer organizations paying ransoms means cybercriminals will look to monetize attacks in other ways.

Cyber insurers are increasingly refusing to pay out for ransomware attacks.

For that reason, most threat actors will follow the same playbook: steal a lot of data and sell it on the dark web while demanding a ransom to not communicate the data breach more publicly.

In the short term, the best possible defense here is to be able to detect a potential attack as it's occurring and prevent successful data exfiltration.

Notable threat actors using double or treble extortion tactics:

- **BlackCat/ALPHV** tools have developed the capability of corrupting/destroying exfiltrated files, leaving the attackers with the only functional copy of the data.
- **Black Basta** use double extortion to encrypt confidential data and threaten to leak it if demands are not met.
- **LockBit** use triple extortion techniques to put more pressure on victims to pay a ransom.
- **BlackByte** use extortion techniques on the dark web to allow the victim to pay to remove their data, and for other threat actors to purchase it.
- **Yanluowang** (associated with LAPSUS$) compromised an employee's VPN account and claimed to have stolen up to 55GB of data.

"YOU CAN'T CONTROL WHAT HAPPENS IN THE CYBERCRIMINAL ECONOMY, BUT YOU CAN CONTROL HOW YOU DEFEND AGAINST THE TECHNIQUES THREAT ACTORS ALL HAVE BECOME RELIANT ON. THE KEY TECHNICAL DEFENSES WORK ACROSS THREAT AND RISK TYPES, SO IT'S BEST TO TAKE A HOLISTIC APPROACH."

Ryan Kalember
EVP, Cybersecurity Strategy, Proofpoint

Ransomware and BEC

Traditionally, Business Email Compromise (BEC) actors and ransomware actors have been viewed as two distinct groups. However, by doing so, we are in danger of complicating an already complex threat landscape.

Yes, certain groups have specialties, skillsets and infrastructure that lends itself to either style of attack. But for the most part, the basic tactics and techniques used are the same.

So, while ransomware and BEC threat actors may display slightly different characteristics, from a defensive standpoint there is a lot of overlap.

In almost all cases, these types of cybercriminals will gain or buy initial access into an environment using a few methods:

1 – **Email phishing**

2 – **Remote desktop protocol** that allows attackers to take remote control of a computer

3 – **Stealer malware** that can collect authentication tokens/ cookies/credentials

BEC and ransomware actors also often use thread hijacking to insert themselves into legitimate communications.

But whatever the tactics of the day, the fact that there is so much similarity offers organizations a huge advantage when building a defense strategy.

Ultimately, you are trying to stop the same activities, regardless of how a threat actor monetizes an attack in the aftermath.

Once we understand this, threat protection and information protection are no longer two distinct challenges with unique control sets. By rethinking our defenses, we can detect and deter today's biggest cybersecurity challenges – BEC, ransomware, and data theft – much more effectively.

Building a defense for every attack

Today's threat scenarios where actors compromise accounts to steal data cannot be solved with legacy threat and data loss prevention solutions. Tools that look for indicators of compromise using data classification rules are no longer fit for purpose on their own. Defenders should instead look for detection signals that map to attackers' current behavior. For example, identifying multiple logins with the same session cookie can flag an attacker leveraging compromised credentials. If that same user's endpoint then sees the installation of an unusual archive tool (i.e. 7zip or WinRAR), the creation of a gigantic multipart archive, or a large amount of data going to cloud file sharing sites often used by attackers (such as Mega), you can safely say it's time to roll incident response.

Today's ransomware operators are opportunists. Whatever their endgame, they will always look for organizations with weak security controls, and they use techniques that work over and over again. They'll seek out vulnerable VPN devices connected to the internet, an open remote desktop protocol port, or people who are going to click a link or download an attachment in a phishing email. And they know that the latter is by far the easiest to find.

That's why defending against all ransomware, data extortion and BEC attacks – which all leverage the same techniques of compromising credentials, impersonation, user-activated malware, and data – comes down to people.

Malicious payloads are almost always delivered through social engineering – and human interaction is essential for these attacks to succeed. When you protect your people, you strengthen cyber resiliency and reduce the chances of a multitude of cyberattacks seeing success.

If cybercriminals cannot get inside your organization they cannot encrypt files, steal data and interrupt business as usual. So, while there may be no silver bullet in cybersecurity, arming and protecting your people by keeping threats at bay and defending your data is as close as it gets.

How Proofpoint defends against ransomware

Our comprehensive, integrated platforms reduce the risk of ransomware attacks by layering controls to prevent initial access and defend against data loss.

Find out more

proofpoint.com/us/resources/solution-briefs/how-proofpoint-defends-against-ransomware

USING THE PRESENT TO PREDICT THE FUTURE

A LOOK AT TODAY'S THREAT LANDSCAPE – AND WHAT IT MEANS FOR TOMORROW

SHERROD DEGRIPPO
Vice President of Threat Research and Detection

We can only predict the threat landscape of tomorrow when we fully understand the threat landscape of today. By analyzing the latest trends, methods and targets, we can predict how threat actors may evolve and develop their attacks to increase their chances of success.

With this in mind, Proofpoint's Resident CISO, Andy Rose, and Vice President of Threat Research and Detection, Sherrod DeGrippo, sat down to discuss the nature of the threats currently facing organizations – and what this could mean for the future of cybersecurity.

#1: People-focused attacks

Threat actors have been targeting people for some time now. People are the key to access; threat actors know this and leverage them accordingly. Further, expert technical capabilities aren't a requirement when it comes to attacking people. We're likely to see more actor groups emerge with a large spectrum of skills, from super advanced to low tech. The common thread will be effective social engineering — meaning attacks against humans, instead of directly targeting data and machines.

Suggested change: Effective social engineering convinces users to engage with malicious content, facilitating entry into a target environment. This initial access method doesn't require additional knowledge or capabilities like exploiting external-facing vulnerabilities or services and is easier for threat actors to conduct broader targeting in higher volumes. With the human aspect perfected, they will then add code, scripts, workflow tools and more to operationalize, increasing both efficiency and effectiveness. Protections and controls alone are not enough to defend against these tactics, so security awareness must be prioritized going forward.

#2: The weaponization of trust

The SolarWinds attack left many blindsided and saw the issue of trust thrust into the spotlight like never before. Its customers, including Microsoft, FireEye and the US Government had every reason to trust the company right up until they didn't. And by then it was too late.

Incidents like the SolarWinds compromise — and the Kaseya ransomware attack — have increased awareness of threats to software supply chains. Threat actors can weaponize trusted third-party services to gain access to an organization and steal information, degrade functionality, or disrupt services. As outsourcing increases and stacks grow ever more complex, it's almost impossible for CISOs to guarantee that everyone in the chain is as diligent about cybersecurity as they should be — they must trust third parties are doing due diligence to protect against attacks.

This may drive a tension, with CISOs seeking to consolidate and simplify the supplier network just as the business decides to move from a 'just in time' supplier model to a 'just in case' one – increasing the supplier base and inviting in smaller partners. Security teams will certainly need to justify their position of partnering closely with a few vendors while CEOs and finance teams push for lower prices and spreading of risk.

AS OUTSOURCING INCREASES AND STACKS GROW EVER MORE COMPLEX, IT'S ALMOST IMPOSSIBLE FOR CISOS TO GUARANTEE THAT EVERYONE IN THE CHAIN IS AS DILIGENT ABOUT CYBERSECURITY AS THEY SHOULD BE

#3: The changing face of insider threats

Insider threats have increased by almost 50% in recent years with annual costs exceeding $15 million. Despite this, it has been traditionally difficult to get buy-in for insider threat management solutions at board level. Employers often feel that their vetting process, coupled with external protections, is enough to keep the problem under control.

But the rise of credential theft has reframed how we look at the issue of insiders. It is now irrelevant whether or not you trust Bob from accounts, because if Bob's credentials are stolen or exposed, you are no longer dealing with him. Once again, there is little technical skill required here, so we can expect a continued rise in this method of attack. Proofpoint researchers have also observed threat actors attempting to recruit employees of target companies to facilitate insider threat-based cyberattacks. When it comes to defence, regular, targeted security awareness training and multifactor authentication are absolutely vital.

#4: Ransomware, data loss and multiple extortion

Ransomware, data loss and intellectual property theft were once standalone attacks, with different methods ultimately achieving each aim. However, over time, these threats began to overlap. Now it is commonplace for cybercriminals to deploy ransomware to encrypt data as well as extracting files to further extort victims.

Now, we're starting to see another layer to this type of attack. Proofpoint threat researchers have observed threat actors attempting to recruit employees of target companies to facilitate insider threat-based attacks. Further, a growing number of threat actors are configuring malware to alert them when it discovers information that may be of value, either for sale or exposure. Once alerted, threat actors will step in manually to assess the highlighted data before deciding on the most profitable next steps. With a single errant click or reused password potentially opening organizations to a chain of attacks, the need for an ingrained security culture will only grow more pressing.

#5: The growing threat of hostile nation states

Think of nation state attacks and you probably bring to mind the big four: China, Russia, North Korea and, Iran. Other countries are expanding their nation-sponsored cyberespionage capabilities and we will likely see India, Pakistan, and other countries, continue to build and improve their programs. Geo-political tensions have also seen others such as Taiwan come into visibility due to ongoing geo-political events. The Middle East is another emerging hotspot as many of the big powers look to diversify economies and play a bigger part on the world stage.

While most organizations will never come into the crosshairs of a nation state, the more action there is on this battlefield, the greater the scope for collateral damage – whether that's system and network outages, or vulnerabilities passed on from a third party.

This puts even greater pressure on CISOs to have visibility into their organizations and work closely with their executive leaders to implement a solid security program.

Understand threat actors and their tactics in our 2022 Social Engineering report

Did you know? Threat actors:

- Build trust with intended victims by holding extended conversations.
- Make use of existing conversation threads between colleagues.
- Expand abuse of effective tactics such as using trusted companies' services.

proofpoint.com/us/resources/threat-reports/2022-social-engineering-report

Your people are the most critical variable in today's cyber threats

Learn more in our 2022 Human Factor webinar.

proofpoint.com/us/resources/webinars/human-factor-2022


Proofpoint
POWER Series
Powering up the security community to protect people and defend data.
Hear from our guest speakers and get the latest cybersecurity insights from our experts in our POWER Series of monthly webinars.
Watch on-demand
go.proofpoint.com/PowerSeries
proofpoint.

Protecting people

The new perimeter

MATT COOKE
Director,
Product Marketing,
Proofpoint

ADENIKE COSGROVE
VP, Marketing
EMEA, Proofpoint

OVER THE LAST DECADE, WE'VE WITNESSED A LOT OF CHANGE IN THE CYBERSECURITY WORLD. THIS DECADE HAS INTRODUCED MOBILITY, MIGRATING TO THE CLOUD AND THE NEW "WORK FROM ANYWHERE" REALITY. WITH ALL THE CHANGE WE'VE SEEN IN THE LANDSCAPE, THREAT ACTORS HAVE ALTERED THEIR TECHNIQUES, LEVERAGING NEW TRENDS AND HOW THEY TARGET. BUT THROUGH IT ALL, THE BIGGEST RISK REMAINS THE SAME: PEOPLE.

Today's top cybersecurity risks are people-centric. Here are the three most common attack types:

Ransomware frequently starts with email that includes an attachment or a link that downloads a malicious file. Cyber criminals want to get inside your organization to collect data and understand the infrastructure before they launch their ransomware attacks.

Business email compromise (BEC) includes phishing, email fraud and social engineering tactics. Cyber criminals are spoofing identities of trusted individuals and suppliers. They're sending simple emails without malicious links and focusing on social engineering to trick your people into wiring money or sending sensitive data.

Data breaches are typically due to one of the following three types of users:

- A malicious user who shares data on purpose
- A careless user who doesn't understand the impact of sharing data
- A compromised user who has fallen victim to an attack and been tricked into sharing data

Figure 1. Throughout the evolution of the cybersecurity industry, cyber threats have continuously targeted people. Find out what else is new for 2022 in our threat landscape webinar.

	2012	2017	2022
MEGATREND	Mobility/BYOO	Cloud	Working from anywhere
DOMINANT CYBER RISKS	Data breaches sercure, payment card theft, espionage, compliance	Automated ransomeware, banking trojans	Big game ransomware, BEC, leavers taking data
BIGGEST RISK	PEOPLE Hackers penertrate secure networks by attaching the weakest links in cyberspace, human beings	PEOPLE 94% of malware comes via email, phishing involved in most breaches	PEOPLE 85% involved a human element, just 3% involved a technical vulnerbility

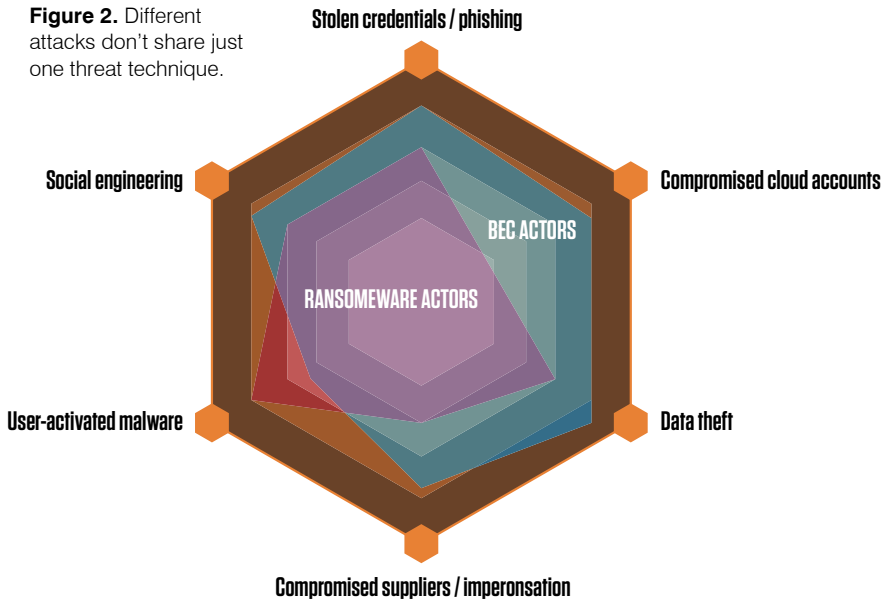
Understand the impact of social engineering on your people

Cyber criminals are using a combination of techniques to gain access to your organization, including impersonating your employees and suppliers. They want to gain access to accounts with credentials — and, if they succeed, they can gain the trust of your workforce.

Ransomware actors also use social engineering to spoof trusted apps and access to steal data. This is why it's so important to understand the impact of social engineering on your people.

Malicious actors work to get your people to run their code for them, hand over credentials to them, and in the case of BEC, transfer funds or data to them. They try to trick people into doing all the hard work for them, so they don't need to "hack in" at all.

Figure 2. Different attacks don't share just one threat technique.



Protect your people: email first

Most cyber attacks today start with a phishing email. And most ransomware campaigns begin with a simple email. For example:

- An employee receives a seemingly innocent email spoofing the identity of a trusted individual such as a colleague or supplier.
- They click the link in the email or open an attachment that runs malicious code.
- Cyber criminals then gain access to the organization's infrastructure, systems, user credentials and important data.
- Eight weeks later, cyber criminals deploy the ransomware activity and cause widespread disruption to the organization.

It's time for organizations to "shift left" and move up the attack chain with their email security so they can prevent malicious attachments from even entering employees' inboxes.

The days of deploying the same controls for all employees are over. The threat profile for each employee, department, team, job role and access to controls is entirely different. In part 1 of this blog series, we covered the evolving threat landscape and how today's top cybersecurity risks are people-centric. This post will discuss how to choose the proper protection for the right people and why it's so important.

Learn more

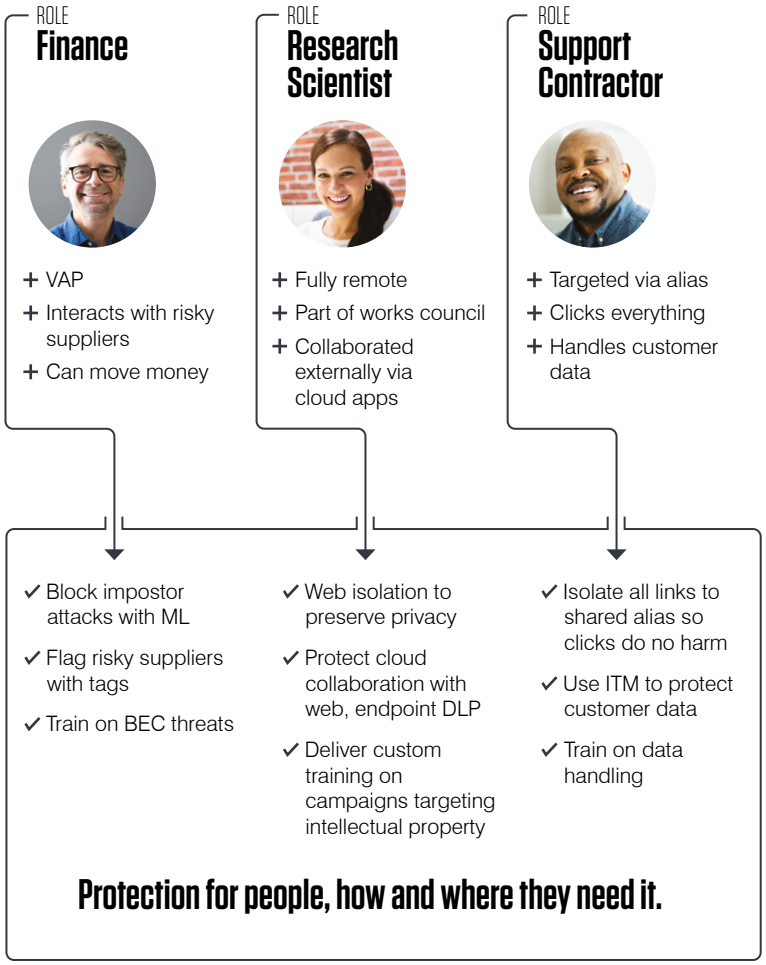
Learn more about how to protect your number one threat vector and identify your organisation's VAPs in our webinar, "Protecting People: The New Perimeter."

proofpoint.com/us/resources/webinars/protecting-people-new-perimeter

How do you protect your people?

Criminals have different motivations for targeting different people in your organisation, so it's important to understand who your Very Attacked People™ (VAPs) are. Who is vulnerable? Who is likely to be attacked? Who has privileged access?

When you understand who does what in your organisation, and why they might be on attackers' radar, you can implement defences that work against the threats that target specific job roles. People are complex and different. Let's look at three examples:



INCREASE YOUR DEFENCES IN THE INITIAL STAGES OF THE ATTACK CHAIN BY PROTECTING YOUR NUMBER ONE THREAT VECTOR —EMAIL SECURITY

Stop malware from reaching your people and increase operational efficiency

Security controls often focus on endpoint detection and response by remediating attacks that have already broken through defences. The early phase in the attack chain is often neglected, but it's so important to prevent attacks before they cause damage.

Increase your defences in the initial stages of the attack chain by protecting your number one threat vector — email security. If you block more threats upfront and have fewer emails reaching users' inboxes, there will be fewer phishing reports for your IT teams to review. Also, because your organisation will spend less time addressing attacks that have slipped past defence, you can improve your operational efficiency.

Consider PerkinElmer, Inc., which was able to block 99% of threats from getting through. Now, it's teams can work more efficiently because they're spending far less time assessing a flood of cyber threats.

"Financial hacking groups targeted us, putting personal credentials at risk. Ransomware threats are real. Our spam and antivirus solutions weren't adequate anymore… Proofpoint TAP (Targeted Attack Protection) helped tremendously… It reduced malicious emails, attachments, and URLs getting through by 99%."

JIM FORSYTH
PerkinElmer's senior network engineer, global IT infrastructure.

Protecting your number one threat vector with a platform approach

Setting up effective defences to deflect threats early in the attack chain reduces your risk profile. Your people can't click malicious links or download malicious files if those threats never reach their inbox. A targeted, platform approach to email security can help. It includes:

1. Implementing controls to block threats from entering your organisation by email. Checking the authenticity of emails helps to block impersonation attempts.
2. Increasing user resilience by educating your people. If an email does get through, are your people trained to make sure the email is legitimate? Do they know to triple check that the attachment or link isn't malicious before they click or open it?
3. Using post-delivery remediation, so if the user does click a malicious link, these unknown URLs can be isolated at the time of the click, preventing malware from entering your organisation.
4. Building automation into the workflow to improve operational efficiency. If a user reports a malicious email, that email can be pulled out automatically from everyone's inbox.

Figure 3. The platform approach to protecting your people.

BLOCK | AUTHENTICATE

REAL-TIME PREVENTION & PROAVTIVE ACTIONS

Detect & prevent initial infection

EDUCATE

AWARENESS, TRAINING & CULTURE

Build user resilence

ISOLATE | AUTOMATE

POST-DELIVERY REMEDIATION

Migrate & recover from lateral movement & persistence

How human behavior impacts cybersecurity...

THE PEOPLE PROBLEM

Over 90% of cyber attacks require user interaction, meaning simple actions – errant clicks, misused passwords – can have severe consequences. With the stakes this high, the need to eradicate these behaviors cannot be understated.

ANDREW ROSE
Resident CISO, EMEA, Proofpoint

DR. BJ FOGG, PHD
Behavior Scientist at Stanford University

To get to the heart of the issue, Proofpoint Resident CISO, Andy Rose, chatted with Dr. BJ Fogg, PhD, to discuss the science behind behavior and how habits can be made and broken. Dr. Fogg is a best-selling author and creator of the Fogg Behavior Model. Here are the key highlights of their discussion.

ANDREW ROSE

I'd like to start off by asking you to explain the Fogg Behavior Model and the concepts that underpin it.

BJ FOGG

Absolutely. The Behavior Model is a universal model for all behavior types of all ages and all cultures. The model demonstrates that behavior happens when motivation, ability and prompt come together in the same moment. That's the motivation to do that behavior, the ability to do the behavior, and the prompt to do the behavior.

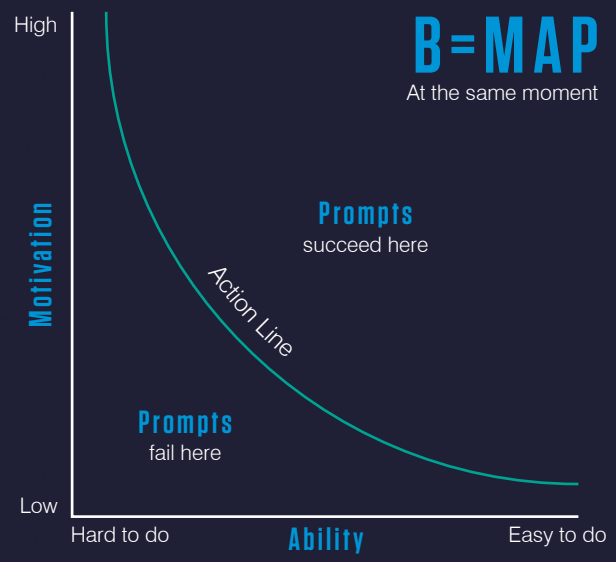


Figure 1: The Fogg Behavior Model - behaviormodel.org

Let's say you want somebody to donate to the Red Cross. If someone is super motivated to do so, and it's easy to do, there's a high likelihood that they will do so when prompted. Now say somebody doesn't like the Red Cross and it's hard for them to donate. Then, they are unlikely to do so when prompted.

Between the ranges of motivation and ability is a threshold called the action line. If someone is anywhere below the line, when prompted, they don't do the behavior. And if they're above, they do. That, in short, is the Fogg Behavior Model.

All specific human behaviors come down to motivation, ability, prompt. If any one of those is missing, the behavior will not happen.

You can really dial it in. We need to make it easier to do, we need to increase motivation, we need to prompt people. It may be that there's enough motivation and enough ability, but no prompt. With this model you can analyse and decide on what's missing.

"...SAYING, "BE CYBER SAFE!" IS A GENERALIZATION. INSTEAD, YOU NEED TO BE AS SPECIFIC AS POSSIBLE"

B = M A P **Behaviour = Motivation Ability Prompt**

ANDREW ROSE

You also wrote a book on the same subject, Tiny Habits. I know it's intended to help individuals change their own behavior, but what do cybersecurity professionals have to do differently to apply this model en masse?

BJ FOGG

There's a different way of thinking about it at scale, but it still comes down to what is the specific behavior we want people to do. And where do people stand in terms of motivation, ability, prompt, and what's lacking to get people to do — or not do — these behaviors. Because you can go in both directions. You can add a prompt or increase motivation, but you can also remove a prompt or make something harder to do.

But either way, specificity changes behavior. So, saying, "be cyber safe!" is a generalization. Instead, you need to be as specific as possible — when you see this kind of thing in this kind of email, do this specific behavior. You need to almost overexplain.

If I had to pick one thing to focus on after specificity, it would be how can we change the difficulty of this behavior to encourage or discourage certain actions. Sometimes we can't change motivation very reliably, but we can make things easier or harder to do — and we can do that at scale.

ANDREW ROSE

Let's talk about the motivation side. We're always telling people what to do, how to do it, and what to look for. But commonly, training these days tends to leave out the consequences of a behaviour. How do we bring motivation and consequences into a security awareness program without overdosing on punishment and killing morale?

BJ FOGG

You need people to align a required behavior with something a user already wants — a motivator. This could be a promotion, status, looking good to their kids and so on. We see this all the time. For example, people don't want to walk on a treadmill necessarily, but they want more energy and improved health.

So, the key is to find something they already want and align your desired behavior with that. Where that's not possible, you need to shift the ability or the prompt component and use those levers. But if you can — this is maximum number one in my book — help people do what they already want to do.

ANDREW ROSE

Does that link back then to the popularity of gamification? Is that a way to create a desire to do something?

BJ FOGG

Yes. It is possible to create ways to motivate. And often that's called gamification. It can be done well, and it can be done poorly. For example, I'm not a fan of leaderboards. Because how many people feel successful when there's a public leaderboard?

One, maybe two. The vast majority feels unsuccessful. So, you need to be careful with the techniques you use to lift motivation and make sure they have broad appeal.

ANDREW ROSE

Now, let's talk about prompts. What tips can you give us on how to create effective and enduring prompts that people will continue to engage with?

BJ FOGG

That's a hard question. There's no magical way. If you're prompting somebody over and over, they can quickly become blind to it, so prompts must be well timed. You don't want to prompt somebody to do something when they can't do it. If they are super motivated to take a training module, but they can't at the time they receive your prompt, that can be frustrating. So, ideally, you're prompting a person when they're both motivated and capable.

With a large population, then it gets trickier. So, you need to do the best you can with the information you have and act on it accordingly. Let's say there is a cybersecurity incident at another company and it's all people are talking about. Guess what? People are going to be more motivated than usual. And if you have them block off some time on their calendar, they have more ability to do it.

ANDREW ROSE

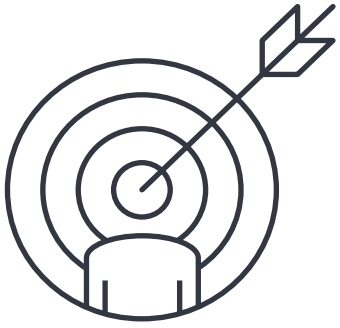
To touch on content again, lots of security professionals are creating it to communicate prompts and awareness messages. How can they create content that recipients will want to come back to again and again?

BJ FOGG

Let me start with what not to do. I call this the "Information-Action Fallacy": If we just give people information, that will change their attitude, which will then change their behavior.

This sounds very logical, but it's not really what works in the long run. Why? Because people believe what they want to believe. Information does not reliably change attitudes. And even if it does, that doesn't reliably change behaviors.

So, it's better to take a behavior and align it with what they already want to do. That way, you don't necessarily have to first change attitudes to change behaviors. So, to answer your question, when people do a behavior and feel successful that then changes how they think about themselves.



ANDREW ROSE

That's why it's really important to have a feedback loop. If someone reports a phish to the security operations center, or they do the right thing, you really want to be the acknowledging that as quickly as you can, right?

BJ FOGG

Yes, the timing of that feedback matters a lot. You can't wait 30 days and then offer a little badge or acknowledgement. That's an incentive but it's not a reinforcer. The emotion, the feeling of success, needs to happen very quickly.

ANDREW ROSE

How about measurement? If you're trying to create a culture of security, how do you create a dashboard or a metric that can be reported up to the board to show your success?

BJ FOGG

Well, certainly there's quantitative measurements we can do with digital systems. But I'm not an expert on that. From a psychological perspective, what you are left with is self-report. I would certainly look at measuring a shift in identity this way. One question I've used for over ten years in the Tiny Habits program is to say, 'I'm the kind of person who…' and let people fill in the blank. This is a good way to measure people's confidence or self-efficacy over time.

"...IT'S REALLY IMPORTANT TO HAVE A FEEDBACK LOOP. IF SOMEONE REPORTS A PHISH TO THE SECURITY OPERATIONS CENTER, OR THEY DO THE RIGHT THING, YOU REALLY WANT TO BE THE ACKNOWLEDGING THAT AS QUICKLY AS YOU CAN"

ANDREW ROSE

BJ, it's been an absolute pleasure talking to you. To close out, do you have any final takeaways or recommendations for the security awareness people that are reading this?

BJ FOGG

Yes. The good news is there's a system behind human behavior. You don't have to guess. You can systematically analyze, you can systematically design, you can test and iterate and improve. And systems give you confidence in what you're doing. You don't have to wonder if you're on the wrong track. You just learn the system and apply it.

MANAGED EMAIL SECURITY

Security is a full-time job and email remains the No.1 threat vector to organizations today. Proofpoint Managed Email Security takes care of the protection of your people against advanced email threats so your employees can focus on other priorities.

Find out more

proofpoint.com/us/products/premium-security-services/managed-email-security

proofpoint®

KEY FINDINGS FROM THE 2022 VERIZON DATA BREACH INVESTIGATIONS REPORT (DBIR) UNDERSCORE THE ROLE OF THE HUMAN ELEMENT IN DATA BREACHES

TIM CHOI
VP, Product Marketing,
Proofpoint

Verizon recently released its latest "Data Breach Investigations Report" (DBIR)[1], offering the latest insights into how threat actors are operating and who they're targeting, and which attack methods are delivering results. This is the 15th annual DBIR, and the report kicks off with an acknowledgement of how "extraordinary" the past year has been, especially when it comes to cybercrime.

The report's authors write: "From very well publicized critical infrastructure attacks to massive supply chain breaches, the financially motivated criminals and nefarious nation-state actors have rarely, if ever, come out swinging the way they did over the last 12 months."

That statement no doubt hits home with most security specialists — and we certainly know our customers have been busy trying to shore up their organization's defenses against a rising tide of business email compromise (BEC) campaigns, ransomware attacks, data breaches, and more.

We'll take a look at a few key findings from the 2022 DBIR to help you assess the challenges and opportunities ahead for your organization as you work to build a sustainable security culture and drive positive behavior change among your users.

The dataset

This year, Verizon analyzed 23,896 incidents across roughly 20 different industries that occurred during the time frame for analysis — from 1 November 2020 to 31 October 2021. Of those incidents, 5,212 were confirmed data breaches.

The 2022 report also marks the third year that Verizon has analyzed incidents and presented them from a macro-region perspective to provide "a more global view of cybercrime."

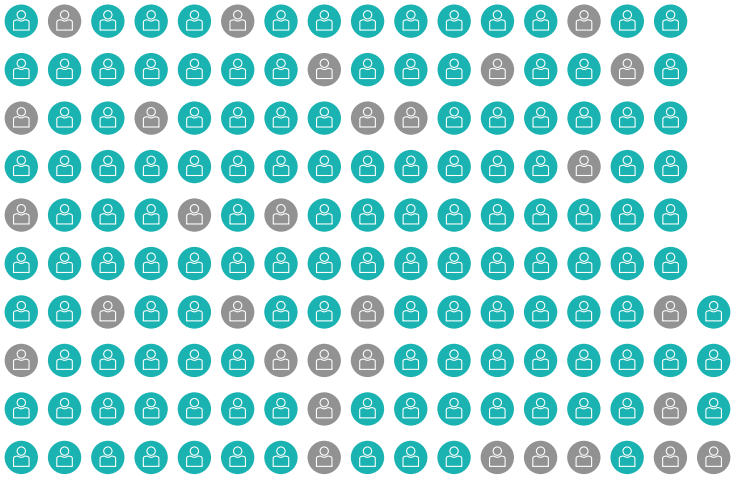


Figure 1. The human element in breaches (n=4,110); each glyph represents 25 breaches. (Source: 2022 DBIR.)

Key finding #1:
82% of breaches involved a human element

This might be considered a positive trend if the percentage still weren't so terribly high. In last year's report, this figure was 85%. The DBIR's authors note that changing human behavior is what's needed to help lessen the role of the human element in driving breaches — but they also acknowledge that doing so is "quite an undertaking" for organizations.

Targeted and data-driven security awareness training for users is a must, of course. Even more critical is adopting a people-centric security strategy, which can help your organization manage security risk more effectively by focusing on threats that target and exploit people.

A people-centric approach to security helps you understand how your people are targeted by threats, how they work in high-risk ways and how they can access valuable data. Developing this approach includes identifying the Very Attacked People™ (VAPs) in your organization. Once you understand the threats they face, and how they are being targeted by attackers, you can implement appropriate controls that will protect them — and your business.

Key finding #2:
Ransomware breaches increased 13% in 2021

Maybe that doesn't sound like much, until you consider that this increase is as big as the last five years combined, Verizon reports. Also, these attacks can be very costly and disruptive for organizations — not to mention society when critical infrastructure is the target.

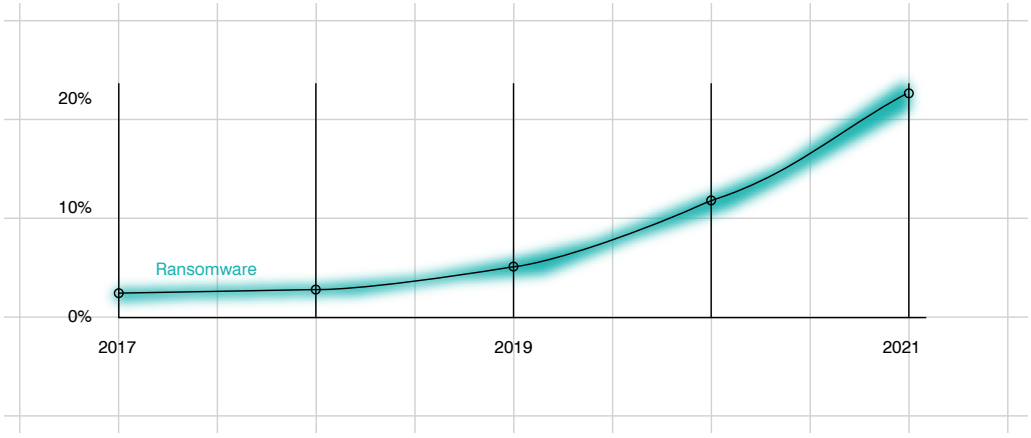


Figure 2. Ransomware over time in breaches. (Source: 2022 DBIR.)

However, the DBIR does offer a reminder that ransomware is "at its core, simply a model of monetizing an organization's access" — and you can reduce your exposure to these attacks by blocking what the report refers to as "the four key paths" to your security estate: credentials, exploiting vulnerabilities, botnets and phishing.

Research Proofpoint conducted for our "2022 State of the Phish" report found that 78% of organizations experienced email-based ransomware attacks in 2021. Our threat researchers also identified 15 million phishing messages with malware payloads that have been directly linked to later-stage ransomware.

Improving your email defenses and providing effective security training can go a long way toward reducing your organization's exposure to phishing. A robust email protection solution can help on both fronts; an email gateway that catches both known and unknown threats, and lets you automatically tag suspicious email to help raise user awareness.

Key finding #3:

62% of system intrusion incidents can be tied to supply chain breaches

Like ransomware attacks, supply chain incidents are increasing. And, as the 2022 DBIR underscores, "compromising the right partner is a force multiplier for threat actors."

DBIR defines supply chain breaches as a sequence of one or more breaches chained together — and one example of a breach that could launch such a sequence is "a breach where a partner is compromised and either a set of credentials or some trusted connection is used to gain access."

RESEARCH PROOFPOINT CONDUCTED FOR OUR "2022 STATE OF THE PHISH" REPORT FOUND THAT 78% OF ORGANIZATIONS EXPERIENCED EMAIL-BASED RANSOMWARE ATTACKS IN 2021

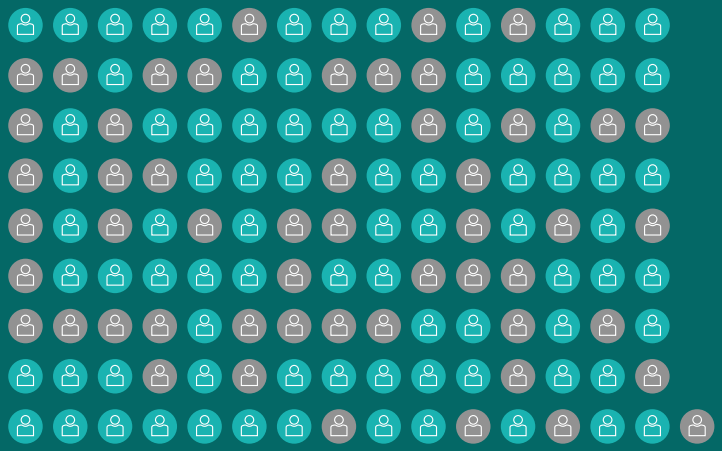


Figure 3. Partner vector in system intrusion incidents (n=3,403); each glyph represents 25 incidents. (Source: 2022 DBIR)

BEC attacks are a method of compromise that take advantage of the complexity of an organization's supply chain. Attackers use BEC scams, which rely heavily on social engineering tactics and include supplier invoicing fraud, to target vendors and other third parties an organization does business with. And, if the attackers succeed at compromising and impersonating trusted vendors, then they're likely well on their way to compromising other entities in the supply chain.

Speaking of phishing scams: It's worth noting that phishing still dominates among social engineering attack techniques, according to the DBIR. The report's authors write, "If you wonder why criminals phish, it is because email is where their targets are reachable."

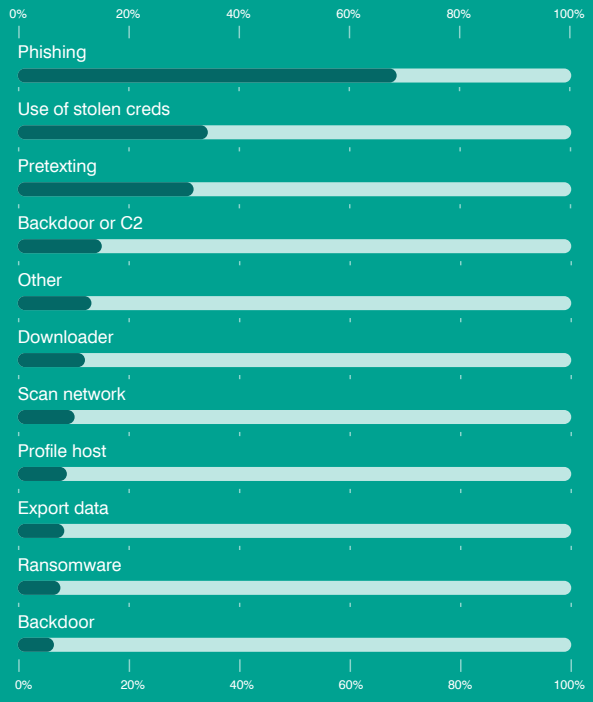


Figure 4. Action varieties in social engineering breaches (n=1,063). (Source: 2022 DBIR)

The DBIR's findings also complement research for Proofpoint's "2022 State of the Phish" report, which found that phishing attacks, including hyper-targeted campaigns like BEC and spear phishing, were up across the board in 2021, compared with 2020.

Keep on reading — there's more to learn

Today's threat landscape is dynamic and complex, and to keep pace, security pros need to stay on top of the latest industry research. So, in addition to reviewing the latest DBIR report from Verizon, we encourage you to check out these resources from Proofpoint:

2022 State of the Phish Report

proofpoint.com/us/resources/threat-reports/state-of-phish

2022 Voice of the CISO Report

proofpoint.com/us/resources/white-papers/voice-of-the-ciso-report

(1) verizon.com/business/resources/reports/dbir/

BUILD A SUSTAINABLE SECURITY CULTURE THAT DRIVES BEHAVIOR CHANGE

SARA PAN
Product Marketing Manager,
Proofpoint

PEOPLE ARE THE NEW PERIMETER—ANYONE CAN BE A TARGET, AND ANYONE CAN UNDERMINE THEIR ORGANIZATION'S SECURITY POSTURE WITH ONE SLIP-UP OR MALICIOUS ACT. LEARN HOW TO FLIP THE SCRIPT AND TURN THEIR ORGANIZATION'S BIGGEST ATTACK SURFACE INTO A CRITICAL LAYER OF DEFENSE.

Drive behavior change by building a systemic and sustainable security culture that's customized to your organization. Many programs aren't inspiring lasting change. Annual training won't prompt most users to adopt a security mindset for the long term. Building a robust security culture will.

IF EMPLOYEES BELIEVE THAT CYBER THREATS ARE A MATERIAL RISK TO THE ORGANIZATION'S SUCCESS AND COULD AFFECT THEM PERSONALLY, THEY'RE MORE LIKELY TO CHANGE THEIR BEHAVIOUR.

What is a security culture?

When an organization has a sustainable security culture employees feel they:

- Are responsible for acting to prevent security incidents.
- Understand why cybersecurity is important.
- Are empowered to act when they see something suspicious or make a misstep.

Your aim is to change how people think about security, and build a security culture that:

- Is holistic and continuous — employees are always learning, and they're engaged and vigilant because they understand their role in defense.
- Has cross-functional advocates — support for a security culture pervades the organization, including at its highest levels.
- Creates and sustains expectations — security policies are designed (and enforced) to drive culture norms.

What are the benefits of a strong security culture?

- Improve agility and resilience.
- Employees feel responsible for preventing security incidents.
- Security teams can respond to threats faster and resolve incidents.
- Reduce risk — increased with remote working, cloud migrations, and use of personal devices.
- Pain-free compliance — reduce missteps leading to penalties due to non-compliance.

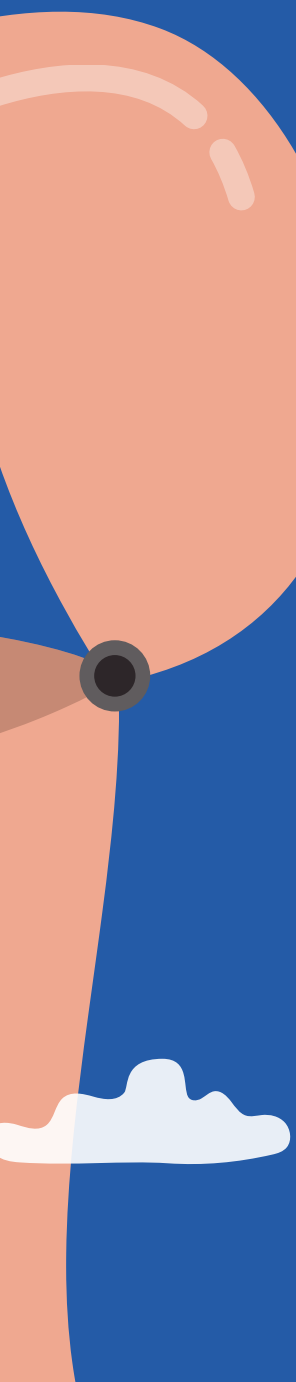


Figure 1. The hallmarks of a strong security culture. (Source: "Beyond Awareness Training" e-book from Proofpoint.)

The challenges to build a security culture — and how to overcome them

Obtaining leadership buy-in

- Map out what-if scenarios for common security incidents to help build executives' awareness about risk and understand the business impacts of an attack.
- Use tabletop exercises to demonstrate what it's like to experience a real attack, like a ransomware campaign.
- Metrics - hard data will appeal to leadership's focus on the bottom line.

Justifying the cost and effort

- The cost of a breach — $4.24 million, on average, according to Ponemon Institute research[2] compared to training costs — significantly less.
- Solutions that automate manual security processes — meaning time and cost savings for the business while reducing risk.

Keeping users engaged

- Explain why security is important to realize the value of being an active defender.
- Make things personal by showing users their risk profile.
- Communicate incidents happening in the "real world" outside of your organization, especially if they impact your industry.
- Make it clear why the information and learning is personally valuable for them — they can use their security awareness skills at home to help protect their loved ones.

Signs of real behavior change

Actions, attitudes and beliefs define an organization's security culture. And when you achieve a well-developed culture, the behaviors and mindsets displayed above, will be evident in your users.

More tips on how to build a sustainable security culture

Download the Proofpoint Beyond Awareness Training eBook. Sell the results to executives and inform them of why your organization must go beyond the same-old security awareness training to instill a security mindset that transforms your biggest attack surface — your people — into a critical layer of defense.

Beyond Awareness Training

proofpoint.com/us/resources/e-books/beyond-awareness-training

Protect people with behavioral analysis and AI/ML for threat detection

MIKE BAILEY
Product Marketing Manager, Proofpoint

GOING BEHIND THE SCENES OF PROOFPOINT'S NEWEST DETECTION ENGINE

We've been using AI/ML (artificial intelligence and machine learning) technology to block malicious and unwanted emails for a long time. But this field is advancing at a stratospheric pace, enabling new capabilities and use cases for organizations to protect themselves. So, it's not just important to do behavioral analysis and AI/ML, but also do them well.

(1) proofpoint.com/us/resources/threat-reports/state-of-phish
(2) ibm.com/security/data-breach

Let's take a deep dive into the specifics of how we use these technologies to tackle email threats and ultimately protect your people.

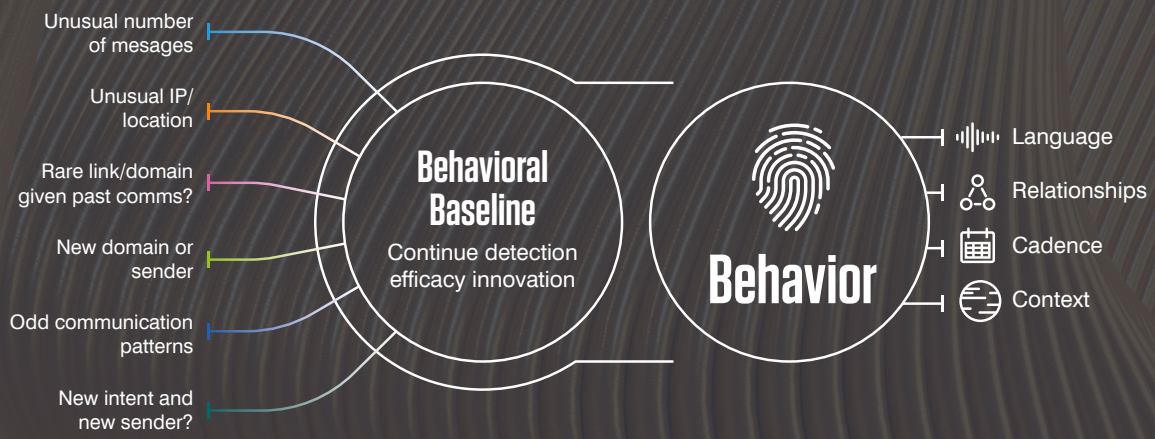


Figure 1. The new Supernova Behavioral Engine analysis uses language, relationships, cadence, and context to detect anomalies and prevent threats in real-time using AI/ML.

New Supernova Behavioral Engine builds on Supernova for BEC

In 2022, we released our Supernova Behavioral Engine to all email security customers globally, at no additional cost and with no additional configuration needed. It better detects email patterns that fall outside of the norm, improving detection of all threat types, from business email compromise (BEC) to credential phishing and much more.

To help your people identify potential threats, the engine will use these signals to determine if a message is malicious:

- Unknown sender, i.e. someone who has never communicated with you before
- Uncommon language or sentiment, such as discussing a financial transaction for the first time
- Uncommon URL or subdomain
- Unusual SaaS (software-as-a-service) tenant, which is often a sign of supplier account compromise
- Unusual SMTP infrastructure, which is likewise indicative of possible account compromise

And it doesn't just include detection. It will also tag messages from uncommon senders using email warning tags with "Report Suspicious" to give the your employees a heads up with valuable context, and allow them to report the message directly to the incident response team or our automated abuse mailbox solution. These behavioral insights can be viewed directly in our Targeted Attack Protection (TAP) Dashboard when messages are condemned.

There is also an improvement in efficacy, while ensuring low false positives. We're committed to transparency, especially given how much vendor noise there is around the use of AI/ML: our current false positive rate is 1 in over 4.14 million - which is industry leading.

SUPERNOVA BETTER DETECTS EMAIL PATTERNS THAT FALL OUTSIDE OF THE NORM, IMPROVING DETECTION OF ALL THREAT TYPES, FROM BUSINESS EMAIL COMPROMISE (BEC) TO CREDENTIAL PHISHING AND MUCH MORE

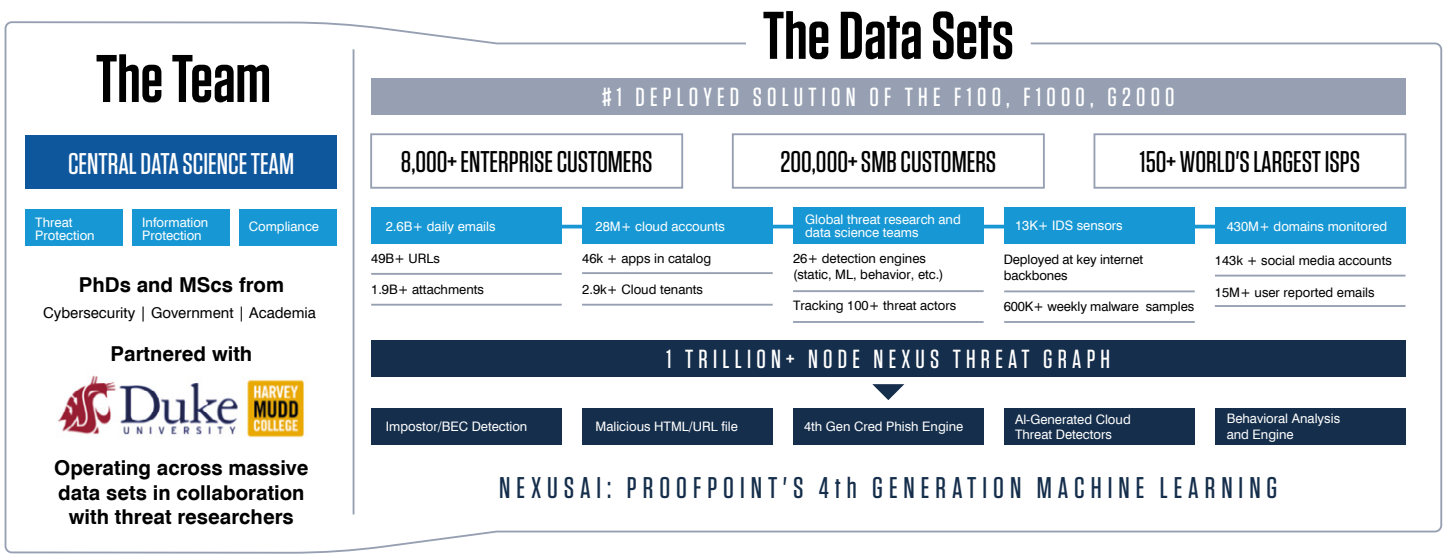
A leading data science team with some of the largest global cybersecurity data sets

Our centralized data science team has been using advanced techniques for more than 20 years to detect and stop advanced threats. The team works across all of our product lines and includes professionals with advanced degrees in cybersecurity, government, and academia. We partner with Duke University, Washington State University, and Harvey Mudd College among other institutions to ensure our skills and technology are cutting edge.

The Proofpoint Nexus Threat Graph[1] has access to massive cybersecurity data sets across email, cloud, networks, domains and more, meaning our teams can feed and improve our models more effectively. Being the number one deployed solution of the Fortune 100, Fortune 1000, and Global 2000 and having more than 200,000 small and midsize (SMB) customers means we can feed our models with data more quickly and detect threats faster and with greater accuracy.

Without a substantial corpus of data, these models become ineffective at identifying threats and sometimes even counterproductive due to excessive false positives.

Figure 2. We use a centralized data science team working with some of the largest cybersecurity data sets in the world to train our models.

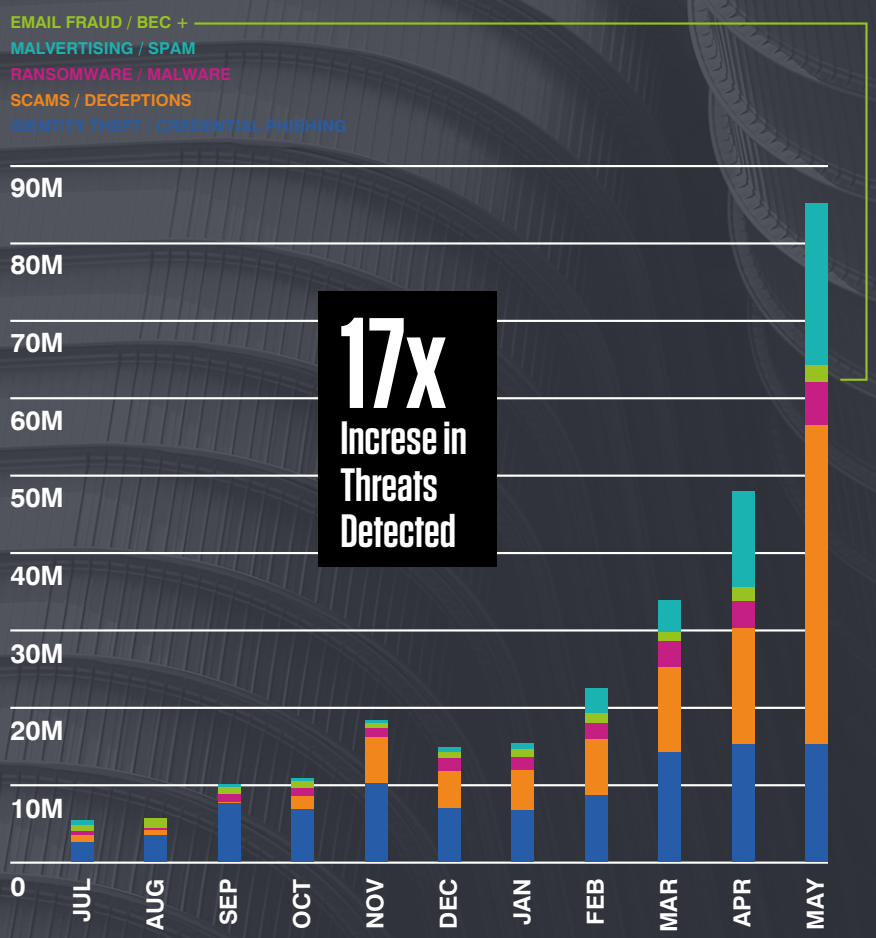


Detection improvements across the board

The results of both engines have been astonishing. Supernova, as part of the Advanced BEC Defense capability, condemns mostly BEC attacks. However, because we've been able to feed the engine so much data, it's been able to learn, adapt and detect much more — including credential phishing, malware attacks and even spam threats.

The engine is also able to better detect and prevent all threat types. When we released the engine in shadow mode, we discovered — in less than four weeks — that it improved detection efficacy against invoicing threats by 6 times.

Figure 3. Supernova, as part of our Advanced BEC Defense capability, now condemns more than just BEC threats; it also effectively stops credential phishing, deceptions, malware, and even TOADs.



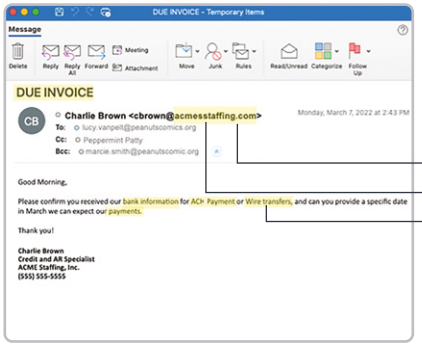


Figure 4. Supernova Behavioral Engine will add additional detection capabilities for BEC attacks, determining the relationship between two parties dynamically.

USER HAS NEVER EXCHANGED LEGITIMATE EMAILS WITH SENDER

OUR NEW SUPERNOVA BEHAVIORAL ENGINE NOW DETECTS THAT THIS IS AN UNKNOWN SENDER TO THE RECIPIENT, IMPROVING THE LIKELIHOOD OF DETECTING AND CONDEMNING THIS ATTACK PRE-DELIVERY

Sample 1

Lookalike BEC threat: improved likelihood of detection

We effectively stop millions of BEC attacks every month. But we're always aiming to raise the bar on detection. In this sample, our existing Supernova for BEC detection engine would have detected the potential lookalike domain and payment language.

Our new Supernova Behavioral Engine now detects that this is an unknown sender to the recipient, improving the likelihood of detecting and condemning this attack pre-delivery. It maps relationships by looking at inputs like cadence, language and context of inbound and outbound messages to determine the relationship status dynamically over time between the two parties.

Even if a dormant, previous sender was compromised and started a fresh attack, the engine would view that communication as anomalous and take a closer look.

Sample 2

Compromised supplier using a URL-based file-sharing threat

Let's say one of your suppliers has a compromised Microsoft 365 account. A threat actor takes over the account, does some research on the specifics of your relationship with the supplier and then sets up a lookalike OneDrive SaaS tenant in an attempt to commit fraud.

The email the threat actor sends comes from a legitimate, common sender, SharePoint, and passes DMARC. In terms of reputation, this email seems legitimate. And the language, a contract, is not unusual given past OneDrive correspondence with this supplier. But there are some tells here that the engine will pick up on.

It will notice the subdomain of the file-sharing URL is different and anomalous and will sandbox the file-sharing URL to inspect the content. That means we can better detect and stop attackers compromising supplier accounts and using lookalike domains or even new subdomains of file-sharing tenants.

NEW TENANT ON A RISKY SAAS PROVIDER

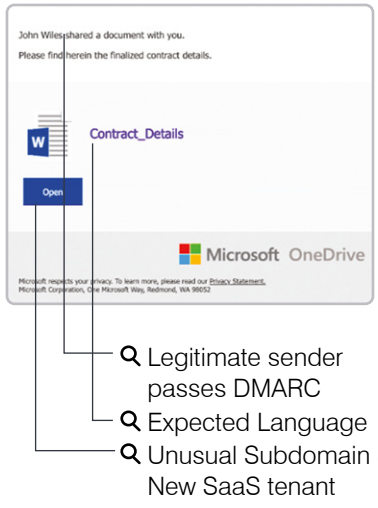


Figure 5. The Supernova Behavioral Engine will better detect compromised suppliers, even if attackers are using a file-sharing site in their attempts to defraud victims.

Proofpoint Detection Ensemble

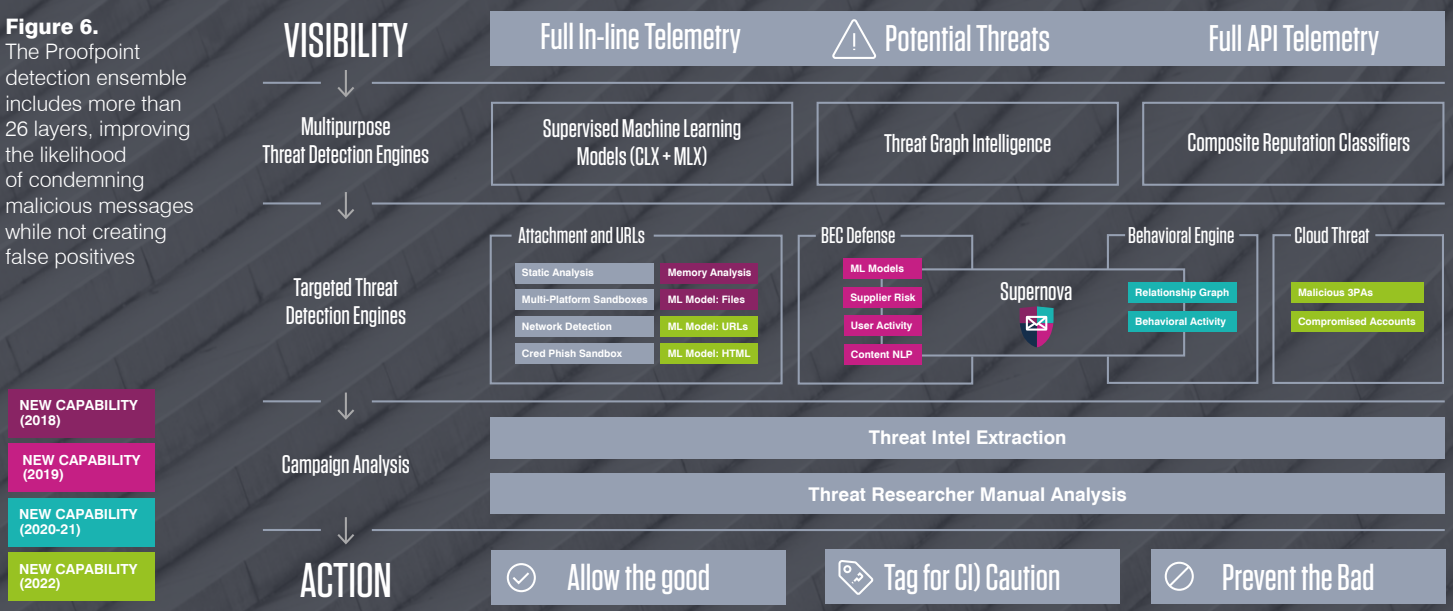


Figure 6.
The Proofpoint detection ensemble includes more than 26 layers, improving the likelihood of condemning malicious messages while not creating false positives

AI/ML and behavioral analysis: part of a broader detection ensemble

Using AI/ML for content inspection and behavioral analysis can improve detection efficacy. Alone, however, we've seen these engines create a lot of noise. That's why they're just a few of the engines we use in our 26-layer detection ensemble.

Broad reputation classifiers combined with our Nexus Threat Graph intelligence frequently stop more than 80% of all malicious and spam messages from ever reaching end users – which could be tens of millions of messages.

We build our attachment and URL sandboxing in-house and use ML models to determine malicious URLs, HTML, files and memory left from potential malware or tampering.

Proofpoint Emerging Threat (ET) Intelligence[2] feeds can quickly identify high-risk IP addresses even if they've only recently become malicious. Our cloud threat data can identify malicious third-party applications or compromised accounts and stop those threats from activating. And our threat intelligence team ties it all together, extracting 7,000+ campaigns annually for a deep dive into emerging, advanced threats to see the latest trends.

(1) proofpoint.com/us/why-proofpoint/nexus-threat-graph
(2) proofpoint.com/us/products/advanced-threat-protection/et-intelligence

Using behavioral analysis and AI/ML to stop phishing attacks

Watch our webinar to learn:

- How Proofpoint uses behavioral analysis & AI/ML to identify threats.
- Pro and cons to each of these approaches.
- How these technologies can evolve and improve.

proofpoint.com/us/resources/webinars/using-behavioral-analysis-and-aiml-stop-phishing-attacks

GAIN KNOWLEDGE FROM DATA TO IMPROVE YOUR SECURITY PROGRAM

- **Implement:** Ensure optimal controls and configuration for baseline protection.
- **Assess:** Understand the threat patterns, trends, and targeting of your Very Attacked People (VAPs).
- **Adapt:** Optimise and prioritise your controls and processes for your VAPs based on targeted threats and the shifting threat landscape.
- **Report and benchmark:** Demonstrate your security progress and posture vs peers.

Learn more about creating a people-centric security program

proofpoint.com/us/products/premium-security-services/people-centric-security-program

proofpoint.

PEOPLE-CENTRIC SOLUTIONS ALLOW THE EDUCATION SECTOR TO DIG DEEPER

In recent years, the education sector has seen a stark rise in cyber attacks, including ransomware, BEC and phishing. Troves of data and multiple attack points have rather predictably placed a target on the back of such institutions. Proofpoint's Matt Cooke, Director of Product Marketing, EMEA, recently sat down with Ed Sleiman, Head of Information Security at KAUST, to discuss these growing challenges — and how Proofpoint is helping to overcome them.

ED SLEIMAN
Head of Information Security,
King Abdullah University of Science
and Technology (KAUST)

A growing challenge

For research universities like KAUST, the need to exchange information as freely and openly as possible makes the challenge to protect it even greater. KAUST is a graduate research university occupying a vast city campus on the banks of the Red Sea. Among the city's 8,000+ residents are professors, researchers, postdocs, students, other university staff and their family members, not to mention some of the world's brightest research minds from over 120 countries. This leaves the security team tasked with enabling open, seamless collaboration with organizations around the world, as well protecting the university's residents in their personal time.

"Our researchers need to work freely. They cannot really have too many restrictions. In their research, they need to be open and collaborative with a lot of other institutions around the world.

What complicates this even more, is the fact that we live in a city. Staff, professors, etc. all want to be able to access everything from their homes — whether that's work-applications, streaming services, or PS5s and Xbox. So, as well as running a campus, we're also running an ISP."

"THE BEAUTY OF THE PROOFPOINT PLATFORM IS THAT IT ALLOWS US TO LOOK AT A RISK AND ALSO THE THREAT COUPLED WITH THE VULNERABILITY. SO, WE CAN TELL WHO IS CLICKING ON A PAGE, WHO IS VULNERABLE, BUT WE ALSO KNOW THE THREATS THEY ARE FACING. BY COMBINING THIS INFORMATION, IT CREATES A BETTER RISK SCORE, MORE HONED TO ALLOW US TO DELIVER EVEN BETTER AWARENESS FOR THOSE WHO ARE MOST ATTACKED"

When protecting such a vast and varied attack surface, perimeter protections and controls can only do so much. KAUST understands that as vast majority of attacks target people, its people are the strongest line of defence when keeping threat actors at bay.

"We've started a program called the human firewall. This basically looks at monitoring and classifying the behaviour of users on the network, then giving them a score that is attributed to their behaviour. So, if a user has never clicked a simulated or real phish or violated any of the security policies then they would have a positive score. This allows us to group users based on risk."

Enhancing the human firewall

Proofpoint's people-centric cybersecurity solutions allow KAUST to dig deeper into user behavior, flag the most attacked and deliver the right training to the right people at the right time. With unique and powerful insights into the university's Very Attacked People (VAPs), KAUST can assess its position in the threat landscape, deploy controls and confidently adapt its security posture.

While equipping its people to protect its data and networks is at the heart of KAUST's security philosophy, it is just one facet of a multi-layered approach. Proofpoint's solutions have allowed the university to complement its human firewall with targeted attack prevention and threat response to block threats before they reach the inbox and quarantine any malicious email that may still get through.

"Before we had Proofpoint, Shamoon 2 hit Saudi Arabia devastating a lot of government and private institutions. One of our human firewalls picked that up in 17 seconds. But let's say this happened in the middle of the night. We don't have a 24/7 human firewall. So, if users were not on the lookout in the morning and clicked on that email, we'd have been dead because that was a zero day. But now, with Proofpoint, that email would be pulled out automatically. So even users that may not be very well trained are protected."

Completing the puzzle

Protecting such a large institution with complex needs is understandably the job of more than one security vendor. But against a barrage of attacks on a daily basis, the university needs real time insight into its current position. It cannot afford to deal with siloed data across disparate systems. For a security solution to work in this environment, it must offer seamless integration to give KAUST's security team a single, at a glance view of its security posture with deep insight into its users at any given time.

"There are tons of security tools out there, from endpoint to application security, to email security. All of these have to work together. One thing that I like about the Proofpoint platform is that it allowed us to complete the puzzle. Proofpoint integrates with out of the box firewalls and a bunch of vendors that are listed on its website. So, we were able to find the vendors that we deal with and then create this integrated platform for us to be able to see exactly where we are in terms of security."

Email is the number one threat vector for inbound threats

It is also a critical threat vector for data loss. Learn how to increase control of your sensitive data with Proofpoint Email DLP and Proofpoint Email Encryption.

Download the data sheet

proofpoint.com/us/resources/data-sheets/email-data-loss-prevention-and-encryption

Get a clear picture of your organization's risk posture

Interested in seeing phishing threats in your environment? In less than five minutes, our assessment can help you better understand your risk posture, helping you uncover threats your email security solution is missing, gain visibility into which people in your organization are being targeted, and see how we can provide your organization with the best integrated, layered protection against evolving threats.

Take our free Email Rapid Risk Assessment

proofpoint.com/us/learn-more/email-rapid-risk-assessment

proofpoint.

CUSTOMER SPOTLIGHT

Global manufacturer forges a stronger security culture with proofpoint

ARISTON
The home of sustainable comfort

The organization

How does a global manufacturer in heating and water heating protect approximately 8,000 employees, 25 production sites, and 26 R&D centers? For Ariston Group, the answer lies in giving its employees the tools and knowledge they need to keep its communications and data fully secure.

The challenge

- Predict, discover and mitigate phishing and other email attacks
- Educate the global workforce on security best practices
- Improve the efficiency of cybersecurity team

The solution

- Proofpoint Security Awareness
- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Email Fraud Defense (EFD)

The results

- Average reporting rate of phishing simulation increased dramatically
- Email threats delivered in users' inboxes substantially decreased
- Decreased unauthorized email attempts with Email Fraud Defense and DMARC reject

The challenge

Enabling employees for more proactive, predictive cybersecurity

Ariston Group is a global leader in sustainable solutions for thermal comfort, components and burners. And like other global enterprises, Ariston Group considers cybersecurity a top priority.

"Our team has a mission to make our architecture more resilient to cyber attacks," said the Ariston Group ICT Security Team Lead. "We identify the appropriate strategies and security controls to mitigate risk in general; plan and implement preventive measures to minimize the risk of threats and their reach; and support incident investigation response and recovery."

Of course, the best way to minimize the impact of threats is to stop them before they can get in. Ariston Group developed a three-year strategy based on a predictive approach, analyzing past events to gain insights, and transforming those insights into action. Empowering employees is a key pillar of this proactive strategy. Ariston Group wanted to educate users and give them the tools and knowledge they need to play an active role in helping to stop threats.

Considering the amount of user mailboxes in its email system, Ariston Group needed an enterprise-grade solution that could detect and stop the latest email attacks. The company was seeking a vendor that could provide not only the solutions and technologies needed for evolving threats, but service offerings to help keep its workforce up to date on the latest best practices.

The solution

Comprehensive security training and email security

The ICT Security Team Lead tested solutions from a variety of leading vendors. They determined that Proofpoint provided the breadth of services and solutions it needed to empower its workforce and apply the most advanced email protection capabilities across its locations around the world.

"We started looking for training offerings, and evaluated the main brands identified by Forrester and Gartner," said the ICT Security Team Lead. "We also needed a solution that gave us tools to help our users evaluate and report suspicious email. And enabling people to provide immediate feedback was key to our remediation strategy. We chose Proofpoint Security Awareness Training because it gave us the strongest combination of these tools and education."

Proofpoint Security Awareness Training provides targeted, threat-guided education. This helps Ariston Group's employees know what action to take when they're faced with an actual threat. The team was especially impressed with its tailored approach that lets the company align its education to specific user roles and vulnerabilities.

"Proofpoint lets us provide specific training for top management, our financial team, and other groups," said the ICT Security Team Lead. "Proofpoint enables us to assign bespoke best practice recommendations to address specific user issues, as well as provide training designed just for new employees."

Proofpoint Security Awareness training also includes extensive language offerings. “In addition to our training activities, we share Proofpoint education content in our internal social networks,” said the ICT Security Team Lead. “And one of the main strengths that Proofpoint offered was its language translation. This allowed us to better support our diverse employees across all our offices.”

As part of its comprehensive email solution, Ariston Group deployed the Proofpoint Enterprise Protection email security gateway and Proofpoint Email Fraud Defense. The company also installed Proofpoint Targeted Attack Protection (TAP) to discover and mitigate ransomware and other advanced email threats that are delivered via attachments and URLs. And with Proofpoint Threat Response Auto-Pull (TRAP), the Ariston Group team can analyze emails and quarantine malicious or unwanted emails after they are delivered to further strengthen security and protection.

“In a way, our approach to protection is inspired by cyber criminals,” said the ICT Security Team Lead “We can look at the TAP dashboard to understand the most frequently used tactics and techniques, and which templates they are using, and which services they are emulating, and then refine our plans.”

“The solution was easy to roll out, and we were able to implement it into production in three months,” adds the ICT Security Team Lead.

“WITH PROOFPOINT, WE CAN DELIVER SECURITY TRAINING THAT IS ALIGNED WITH OUR DIFFERENT ENVIRONMENTS AND CULTURES. WE CAN ALSO STAY UP TO DATE WITH THE LATEST EMAIL PROTECTION CAPABILITIES. AS A RESULT, WE CAN PROTECT OUR ENVIRONMENT AND GROW AND SUSTAIN OUR KNOWLEDGE.”

Ariston Group ICT Security Team Lead

The results

Getting out in front of email threats

With Proofpoint Security Awareness Training — and its broad set of email security solutions — Ariston Group has a comprehensive solution in place. And the company has seen dramatic and measurable results.

"We have seen a huge reduction of risk in terms of malware and targeted attacks," said the ICT Security Team Lead. "Proofpoint is able to identify specific, targeted attacks against our supply chain, and block communication in advance. Proofpoint Security Awareness Training has helped us augment this protection. It improves awareness among our employees and gives them the tools they need to recognize attack techniques and report them."

The Ariston Group team measured the average reporting rate of the phishing simulation in Proofpoint Security Awareness Training. They found that the rate has increased steadily and significantly over three years. This growth shows that Ariston Group employees are more engaged in protecting the company. It also reflects how they have changed their behavior to take on more responsibility in helping defend against threats.

The team also looked at the number of emails that were deemed malicious, suspicious or spam. They did this using PhishAlarm Analyzer, which is part of Proofpoint Security Awareness Training. This tool uses Proofpoint threat intelligence to help the team identify the most serious threats. Within one year, Ariston Group saw a remarkable reduction in threats delivered to its user inboxes.

Proofpoint also provides up-to-date insights into the latest cybersecurity threats. This enables Ariston Group to tailor its training so it can keep up with a constantly shifting threat landscape.

"PROOFPOINT IS A COMPLETE SOLUTION THAT GIVES US FULL VISIBILITY INTO WHAT'S GOING ON IN THE COMMUNICATION STACK, THE PEOPLE STACK AND THE BEHAVIORAL STACK," SAID THE ICT SECURITY TEAM LEAD. "WHEN WE APPLY THAT INTELLIGENCE, WE CAN FIND THE GAPS IN OUR REAL ENVIRONMENT. THEN WE CAN USE THOSE INSIGHTS TO BETTER ALIGN OUR EMPLOYEE TRAINING PROCESSES."

Proofpoint Email Fraud Defense has also helped Ariston Group take more control over its domain to stop phishing attacks. Working closely with a Proofpoint Professional Services consultant, Ariston Group set up Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). Next, the company set up a Domain-based Message Authentication Reporting and Conformance (DMARC) "reject" policy for its domain. As a result, the delivery of unauthorized messages dropped completely over just six months.

"The support we received from the Proofpoint Professional Services team was one of the key factors that led to our project's success," said the ICT Security Team Lead. "Our representative understood our needs and guided us through the technical steps needed to authenticate our external services and platforms."

With its advanced email technologies in place, and a proactive company security culture, Ariston Group is set up for success. The company is confident in its ability to stay ahead of evolving threats well into the future.

Protect your people to fight systemic risk

SYSTEMIC RISK HAS BECOME SOMETHING OF A BUZZWORD IN CYBERSECURITY CIRCLES IN RECENT YEARS. BUT WHILE MANY ARE NOW FAMILIAR WITH THE TERM, ITS DEFINITION AND SCOPE CAN VARY SIGNIFICANTLY.

LUCIA MILICĂ
VP and Global Resident CISO, Proofpoint

Carnegie Endowment for International Peace and the Aspen Institute defines the concept as "the possibility that a single event or development might trigger widespread failures and negative effects spanning multiple organizations, sectors, or nations." The Digital Directors Network, known as a leading voice on the topic, describes systemic risk as "the threat that component failure in a complex system will cascade and jeopardize the much larger system."

Naturally, the more complex a system, the greater the risk that one single event can have a domino effect, cascading far and wide through organizations, supply chains and infrastructure.

Unfortunately, complex systems are often the rule rather than the exception. Most organizations and institutions, including those critical to national infrastructure, operate across a patchwork of new technologies and legacy systems, with in-house, cloud and third-party setups. So, the challenge of protecting these sprawling ecosystems is almost insurmountable.

But with the issue of systemic risk firmly in the spotlight, it's a challenge that CISOs must overcome quickly. The consequences of systemic risk run far and wide, from service interruption and data loss to brand damage and multi-million-dollar regulatory fines. And just one broken link in your chain can expose your business to these repercussions — and much more.

The sprawling impact of systemic risk

The concept of systemic risk is by no means a new one. But as we become increasingly reliant on digital, connected, and multi-layered systems, its scope has increased dramatically in recent years. As a result, there are numerous examples of a single failure putting businesses, services and even lives at risk.

Take the SolarWinds incident. What started as an injection of malicious code within a private organization quickly spiralled to impact the services of government departments and Fortune 500 companies. Soon after, it became a fully-fledged international incident when the U.S. Government responded by imposing sanctions on Russia. And with the company accused of not fully understanding its level of exposure to systemic risk, its current and former board members are still facing legal and regulatory fallout to this day.

But malicious outsiders are not the only threat actors contributing to systemic risk. Another example with potentially much more far-reaching consequences is last year's insider incident at Pfizer. A (now former) employee stands accused of exfiltrating over 12,000 files, some marked confidential, and uploading them to a personal Google Drive.

While the IP heist was stopped in its tracks, the damage that this incident could have done to the COVID-19 recovery is almost incomprehensible. The potential theft of the leading vaccine formula by the Chinese government would likely have sowed confusion and distrust, potentially delaying the global rollout, allowing more time for new variants to develop and increasing death tolls. Clearly, a problem much more extensive than its impact on Pfizer and its shareholders.

While markedly different in their mechanics, targets, and potential consequences, both incidents highlight the pivotal role of people as systemic risk. With over 90% of cyber incidents requiring human interaction, it may take just one click to unleash a world of issues that far exceed the reaches of your organization. When the stakes are this high, it is absolutely essential that your users are equipped for such a responsibility.

The number one risk factor — your people

People are the number one risk factor when it comes to systemic risk, whether they are within your organization or at a third party within your supply chain. It takes just one malicious insider, one errant click or reused password to kick start the domino effect. So, first and foremost, you need total visibility into who is accessing your data — when, where and how.

The more you understand your people and their activity, the more protections you can put in place to help them defend your organization. While vital, this extends beyond perimeter fences and filtering systems. The onus is on security teams to educate employees on their role in exposing organizations and the wider world to risk.

By building a cyber aware culture throughout your supply chain, you can change the kind of behaviors that open the door to threat actors wherever they may originate. This means adaptive, ongoing, and comprehensive security awareness training targeted to those who need it most.

This is no longer just a matter for your IT team. Organizations now have a civic, perhaps even a moral, duty to minimize and mitigate risk wherever possible. As the Chief Justice of the Delaware Supreme Court recently put it, organizations must "demonstrate credibly that they are thinking proactively about systemic risk." If you're not, you could soon face consequences that stretch far beyond the walls of the boardroom.

PEOPLE ARE THE NUMBER ONE RISK FACTOR WHEN IT COMES TO SYSTEMIC RISK, WHETHER THEY ARE WITHIN YOUR ORGANIZATION OR AT A THIRD PARTY WITHIN YOUR SUPPLY CHAIN

Defend your data from the great resignation

Learn how to stop your data leaving with your employees in our article on page 50

THE GREAT RESIGNATION IS INCREASING THE RISK OF DATA LOSS - WHAT CAN YOU DO TO STOP IT?

The market dynamics of the past several years have created a massive undercurrent: employees are leaving — and subsequently joining — organizations at an unprecedented rate. Dubbed 'The Great Resignation', and often referred to as the 'Great Reshuffle', over 47 million Americans voluntarily quit their jobs in 2021 — a new record.

The Great Resignation combined with the work-from-anywhere workplace and cloud adoption has created a perfect storm for organizations trying to protect their most important and sensitive data. At the same time, legacy DLP systems that are on-premise, complex and costly to maintain cannot keep pace with today's modern workforce.

Halfway through 2022, these trends show no signs of abating. And even as employees in the tech sector are affected by recent layoffs, the implication is the same: employee turnover puts sensitive data at risk.

STEPHANIE TORTO
Senior Product Marketing Manager, Proofpoint

SAI CHAVALI
Senior Product Marketing Manager, Proofpoint

Great resignation and insider threats top CISO challenges

According to the 2022 Voice of the CISO report, insider threats increased from the number three spot in 2021 to number one in 2022. With the volume of insider threats increasing 40% in 2022, it's easy to understand why insider threats are top of mind for today's CISOs.

Furthermore, 50% of CISOs state that protecting data has become an increased challenge due to the Great Resignation. As employees leave companies in historic numbers and data volumes increase significantly, it is critical to put the controls in place to protect your most valuable data.

The departing employee

Departing employees can be categorized as malicious or careless users. The malicious user is typically motivated by personal gain and departing employees, who may want to get a jumpstart in their next job opportunity, are a common use case. For example, the departing employee may feel entitled to customer data based on their relationships or to intellectual property given the 'sweat equity' they contributed.

The careless user is well-intentioned but may accidentally exfiltrate data as they leave the company. For instance, a user may inadvertently download sensitive data like financial reports or credit card numbers to a USB while trying to download personal documents.

Understanding a user's motivation is critical to gaining context and determining the best response. Proofpoint believes that a people-centric approach to data loss is needed — one that is content, behavior and threat aware.

50% OF CISOS STATE THAT PROTECTING DATA HAS BECOME AN INCREASED CHALLENGE DUE TO THE GREAT RESIGNATION

Having insight into a user's intentions and behavior helps determine if the actions are a result of a careless user or a malicious user.

Given the potential for financial and brand impact from malicious users, these incidents tend to be widely publicized. There are several recent examples of data loss stemming from departing employees. In November 2021, Pfizer alleged[1] that a former employee exfiltrated thousands of files with Covid vaccine trade secrets as they left the company. Similarly, in December 2021, Qualcom[2] discovered that a long-term employee exfiltrated hundred of files with confidential and proprietary information to his personal accounts before leaving for a new job. In both instances, these long-term employees wanted to take data that would be useful to them as they were headed to their next opportunity.

How to stop data loss from departing employees

An employee gives their notice to leave the organization. The employee works with sensitive customer data and critical intellectual property. Unfortunately, the employee also believes the code and designs are their hard work and belong to them. So, they want to take the sensitive information to their next job. How can you protect your organization?

Fortunately, there are several steps your organization can take. Proofpoint Information and Cloud Security is a cloud native platform that stops data loss, investigates insider risk, and blocks cloud threats. Part of this platform are Proofpoint Insider Threat Management (ITM) and Proofpoint Cloud App Security Broker (CASB), which help you stop data loss from departing employees across managed and unmanaged devices.

With these solutions, you can:

Monitor departing employees – Build a watch list of departing employees. As users give their notice and HR tags them as leavers, ITM will automatically start monitoring these users as risky users, providing visibility into their data activity on managed endpoints.

Detect and prevent malicious users – Policies can be set up for exfiltration of sensitive data via a USB, cloud sync, or an unauthorized website. Departing employees' actions can also be blocked and screenshots can be captured to provide forensic evidence for an investigation. Alerts will be generated for any out of policy behavior for departing employees so the security analysts can react in real-time.

Identify and remediate careless behavior – Identify when users share sensitive files in the cloud, such as through OneDrive, Google Drive, Dropbox, too broadly or simply with unknown recipients (e.g. email address typos). Most customers set up automated remediation policies to protect cloud files in such cases while only allowing collaboration between trusted parties.

Investigate departing employees – Manage investigations, triage alerts and dig deep into the metadata to understand a user's timeline of activity. With departing employees stealing sensitive cloud data, CASB will automatically correlate all their abnormal or risky cloud data activity in the recent past (e.g. their notice period). PDFs and reports of the concerning activities can be easily exported for use by HR, Legal, and other departments that may need to be involved.

Prevent data loss across channels – Gather telemetry across channels – from endpoint, email, cloud, and web – so that you can have a holistic view of incidents and avoid ad hoc, time consuming investigations that require pivoting between different tools. As a result, you will gain visibility and contextualized insights, proactively hunt and respond to threats and work more efficiently to minimize business disruption.

Read more about how to build an information protection strategy that protects your people while defending your data on page 53.

Learn more about protecting your organization from insider threats

Watch our webinar and demo to learn more about how Proofpoint ITM and Proofpoint CASB can help you protect against insider threats.

proofpoint.com/us/resources/webinars/how-stop-your-data-leaving-employees

Learn more about the Cost of Insider Threats in the 2022 Ponemon report

proofpoint.com/us/resources/threat-reports/cost-of-insider-threats

(1) news.bloomberglaw.com/ip-law/pfizer-says-employee-stole-files-with-covid-vaccine-secrets

(2) securityboulevard.com/2022/03/qualcomm-wed-like-our-ip-back-please/

Protecting people. Defending data.

How to build and implement an information protection strategy

JEREMY WITTKOP
Senior Director, Technology Services, Proofpoint

There is no smoking gun in the world of cybersecurity. No single tool, control or protection can prevent every attack. That's why it is vital that IT teams must have the means to identify and safeguard sensitive information – wherever it is and whoever needs access to it.

This is only possible with a comprehensive information protection strategy. One that can classify and ringfence sensitive data, reduce your attack exposure and lower compliance risk. So you can defend your data and protect your people without disrupting your business. To help you achieve these aims and more, here are five key considerations to keep in mind when building and implementing your information protection strategy.

1. Get total visibility

Any successful information protection strategy must be tailored to your business and its risk profile. Off-the-shelf tools may be powerful, but they are not enough alone. So, before looking for solutions, you must first determine what you are trying to accomplish. That means gaining visibility into:

- What you are trying to protect – your customer data, IP, business processes.
- What you are protecting it from – data loss, negligent and malicious insiders, encryption.
- What risks does it face? Accidental exposure, account compromise, IP theft, employee churn.

Only when you know what you wish to achieve can you start to make a business case and build a strategy to achieve it. So, the task now is to work with key stakeholders to demonstrate what is at risk, what it is at risk from and the resources you need to mitigate that risk.

2. Start small

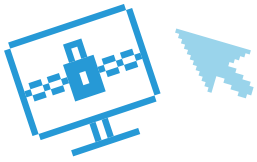
In the early stages of building an information protection strategy, it can be easy to feel overwhelmed by the potential scope of the operation. There is likely a wealth of information you would like to protect, but it's important to keep things in perspective. And remember, perfect is often the enemy of good.

There's no need to stretch your budget over 20 use cases when one will do. If you have the budget to fix one problem right now, start with that. This one use-case can act as a cost-benefit analysis, helping you to start small, prove the concept and then add to your defenses over time.

Customer testimonial

'WE'VE TAKEN A RISK-BASED APPROACH BY GETTING A TECHNICAL SUITE OF PRODUCTS IN PLACE TO PROTECT AGAINST DIFFERENT THREAT VECTORS. IT'S LIKE TRYING TO 'PLUG THE SWISS CHEESE' – WHERE ARE YOU AT RISK AND WHERE ARE YOU POTENTIALLY LOSING DATA?'

Robert McIntyre
Director of Information Security, Tetra Pak.



3. Building versus implementing

Building and implementing an information protection strategy are two very different tasks with very different challenges. There are few businesses out there that can build a strategy without expert guidance. With varying priorities and stakeholders, paralysis by analysis is commonplace. That's why most IT teams need a security expert to say, let's start here, and we can continue to have these discussions, rather than talking for six months before putting anything into action.

The sooner you implement your strategy, the quicker you can access real-world data that will almost certainly influence your decision-making going forward. So, it is always better to get the basics in place and adapt than to spend months planning based on what you think is happening within your organization.

When it comes to implementation, once again, it is important to keep in mind what you are trying to achieve. There is no worth in buying the best available tools if you are unsure what you intend to do with them. But with a clear plan in mind, you can set about configuring tools – email, endpoint, cloud apps, web, on-premises and cloud protections – to defend your data. At the same time, you should also implement the other arm of your strategy to protect your people by flagging risky behaviors and reinforcing security best practices.

4. Changing behavior

While tools and controls are a vital part of any information protection strategy, it is your people who form the first and last line of your cyber defense. Think of cybersecurity technology as your safety net. It's great to have it there, but you don't want to test it out very often.

Instead, you must educate your users to keep your business safe rather than rely on technology for protection. This requires comprehensive and ongoing security awareness training. There's a saying in cyber security – familiarity breeds commoditization. In other words, it doesn't matter how sensitive your data, if your people are working with it day to day, it becomes a commodity.

So, it's essential that you constantly remind them of the severe consequences of failing to protect that data and the role they play in doing so. The more they know about how they should treat information, the less likely they are to expose it to risk and the smaller your attack surface becomes.

5. Ensuring success

Against a constantly evolving threat landscape with users accessing data anywhere at any time, ensuring the success of any cybersecurity strategy is never easy. However, the best thing any organization can do to help its chances is to conduct an honest assessment of its people, processes and technology.

By understanding your strengths and limitations in each of these areas, you can plug the gaps accordingly. For some businesses, this might mean looking to a security partner for nothing but guidance and advice. Others may have the best strategic minds but need more hands at the keyboards. Either way, the key is understanding where you need the most support and seeking it out at the earliest opportunity. Once every piece is in place, you can design and build a strategy to get on with the job at hand – defending your data and protecting your people.

Customer testimonial

OUR ABILITY TO IMPROVE EMAIL DETECTIONS AND THE EFFICACY OF THE BLOCKS WE PUT IN PLACE, HAS MADE A HUGE DOWNSTREAM IMPACT. MORE RECENTLY, OUR FOCUS HAS BEEN ON THE VISIBILITY OF OUR INTELLECTUAL PROPERTY AND HOW WE STOP THE ASSOCIATED LOSS OF DATA – WHICH IS ESPECIALLY IMPORTANT RIGHT NOW. WHILST THE GOAL IS TO PROTECT, IT CAN BE EXPLAINED AS A PYRAMID – WE HAVE TO START WITH VISIBILITY, AND THEN BUILD ON THAT WITH DETECTION, AND THEN WE CAN START TO PROTECT.'

Guy Delp

VP of Global Information Security, Pfizer Inc.

Cure staffing shortages in cybersecurity with automation

The need to increase investment in corporate Security Operations Centre (SOC) teams is intensifying as high-profile attacks become more frequent and sophisticated.

DAVE COOK
Senior Product Marketing Manager, Proofpoint

According to the Identity Theft Resource Center[1], the number of publicly reported data compromises by the end of September 2021 had already exceeded the total number of events in 2020 by 17%. Attackers are becoming more systematic in their targeting and tactics, making security even more challenging.

Recent research[2] from The Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA) found that over the last decade, the cybersecurity professional skills gap has continued to increase, impacting over half of organizations. The top ramifications of the skills shortage include increasing workload (62%), unfilled open job requisitions (38%), and high burnout among staff (38%).

Together, this could mean a difficult situation if companies don't do something soon to help their security teams. But what can they do?

Easing the security team workload

Many corporations are recognizing the need to help SOC teams by investing in ways to decrease their overall workload. 31% of cybersecurity professionals rated "overwhelming workload" among the top three most stressful aspects of their job.

What are the most stressful aspects of your job as a cybersecurity professional? (Percent of respondents. N=489, three responses accepted

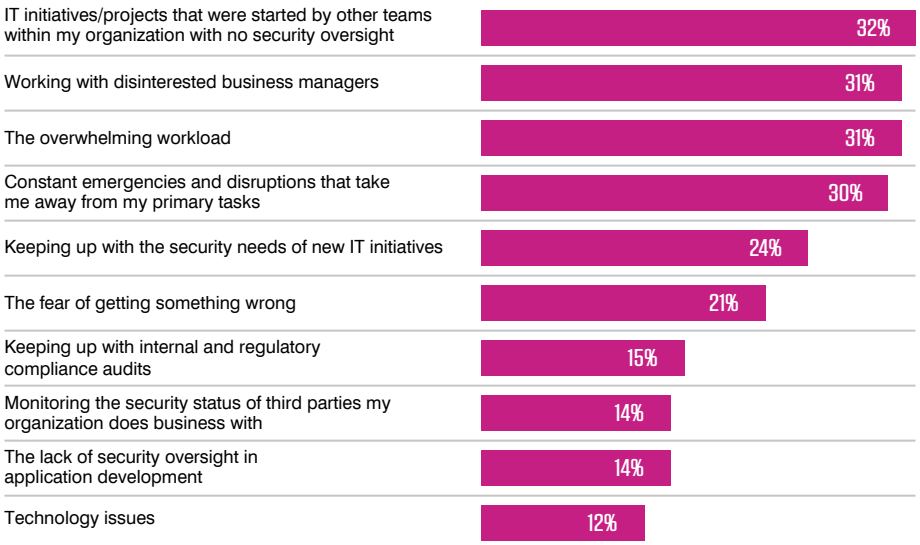


Figure 1. The top 10 most stressful aspects of cybersecurity professionals' jobs. (Source: ESG and ISSA's joint research project, "The Life and Times of Cybersecurity Professionals 2021," Volume V.)

One way that companies are trying to invest more in their security amid staffing shortages is by outsourcing some activities using managed services like managed detection and response (MDR). However, these can sometimes be an afterthought, as corporate budget holders generally have less insight and aren't as invested as SOC teams in recognizing the need.

Another method many SOC teams are turning to is automation, which can ease their workload and improve their security strategy by providing additional information and insights. Automation can improve efficiency by accurately detecting most initial threats, so specialists can focus time on the highest-risk threats hitting the organization.

Automating multiple aspects of email security

Threat detection

The first ingredient to a successful threat detection and prevention system is the ability to accurately detect the threats that target your people before they can become real threats to your organization. These can be as simple as common spam or malware that is relatively easy to recognize, or they can be more sophisticated multi-stage malware attacks or advanced business email compromise (BEC) and supplier risk threats. Effective threat detection can be used to recognize and stop these threats so that SOC teams don't need to worry about additional threats entering their environment.

"WE WERE DROWNING IN PHISHING ATTACKS. WE NEEDED HELP REDUCING NOT JUST THE QUANTITY OF ATTACKS, BUT ALSO THE AMOUNT OF TIME SPENT RESPONDING TO ATTACKS."

Aaron Baillio
CISO, The University of Oklahoma

The University of Oklahoma[3] was feeling the pain of both an increase in the number of attacks and the lack of resources to handle them.

By using automation the university's security team saw immediate and concrete results. 50% - 70% of all email sent to the university was identified as malicious, bulk or otherwise unwanted, and stopped it from being delivered to users. This automatically reduced the SOC team's workload by eliminating the need for security personnel to manually triage or remediate each one of those emails.

Automated remediation

For any threats that do get through the initial detection, an automated abuse mailbox monitoring solution can work together with your end users to remove risks from your organization more quickly.

By using automation in this way, SOC teams can spend their time on manually triaging the more advanced attacks that can be the most difficult and time-consuming to address. Less time spent triaging smaller incidents also means SOC teams are spending more time honing their skills and expertise to become even better analysts.

Deploying automation into your security workflows

It's one thing to speak about the benefits of a robust, automated system, but it's another to put it in place within your organization. Over 50% of survey respondents in the study from ESG and ISSA[2] agreed that security professionals spend too much time on the technical aspects of cybersecurity and not enough time on how cybersecurity aligns with the corporate mission.

This process works best when the automation is fully integrated into existing workflows and security solutions – saving time and improving efficiency.

Decreased workload

Automation can improve workloads by decreasing both the number and complexity of remediation tasks. However, it can also provide more detail about each threat which helps incident responders understand it more quickly and spend less time remediating it. This, in turn, opens up more time for the SOC team to focus on corporate goals.

Having an integrated security platform and managing every aspect of cybersecurity from a single interface reduces the time needed to move from one task to another. The ability to share underlying data, analytics and infrastructure is another benefit, as it helps to enable many automation capabilities.

To summarize, automation can help ease the burden on SOC teams and make them more effective by:

- Reducing workloads by detecting and stopping the majority of incoming threats.
- Remediating threats automatically and more quickly, before they become real concerns.
- Organizing threats and alerting SOC teams, helping them better focus their skills and resources.
- Creating new policies and actions automatically to reduce future threats.
- Making more time and capacity for SOC teams to focus on high-risk threats.

"TODAY, WE HAVE A SINGLE PLACE TO GO TO PROTECT EMAIL USERS, SECURE CRITICAL ENVIRONMENTS AND REACT TO INCIDENTS… THIS LEVEL OF INTEGRATION HAS INCREASED OUR IT TEAM'S PRODUCTIVITY. WE NOW SEE VALUABLE, TANGIBLE RESULTS."

Aaron Baillio
CISO, The University of Oklahoma

Find out more in our Managing the Cybersecurity Skills Shortge eBook

proofpoint.com/us/resources/e-books/managing-cybersecurity-skills-shortage

(1) idtheftcenter.org

(2) The Life and Times of Cybersecurity Professionals 2021, Volume V, A Cooperative Research Project by ESG and ISSA. 2021, The Enterprise Strategy Group, Inc.

(3) proofpoint.com/us/customer-stories/university-oklahoma-controls-phishing-attacks

Protect people. Defend data.

Combat advanced threats. Prevent data loss.
Modernize compliance.

For cybersecurity, information protection and compliance, people are the new perimeter.

People are your greatest asset. They're also your leading source of security risks, data loss and compliance issues. Keep your users safe. Keep your data secure. Keep it all compliant with Proofpoint. No other cybersecurity partner is trusted by more Fortune 500 and Global 2000 companies to protect their people and defend the data they create.

Threat Protection

Email and the cloud are today's primary attack vectors for ransomware, business email compromise, phishing and other threats. Fight back with a people-centric approach that blocks attacks, secures cloud accounts and educates users. Our multilayered, holistic approach helps you:

- Secure the gateway and protect email with threat detection powered by machine learning
- Understand who is being attacked and who's most vulnerable
- Automate incident response
- Change user behavior and help your people report potential threats
- Stop domain spoofing
- Prevent account takeovers
- Prevent web-based threats and secure users' browsing activity

Information and Cloud Security

Data doesn't lose itself. Prevent data loss from malicious, negligent and compromised users by correlating content, user behavior and external threats. Protect your data with AI-powered insight that detects data leaks and streamlines investigations. Our modern solution helps you:

- Prevent sensitive information from leaking through email
- Safeguard cloud apps and protect users from cloud threats
- Connect the dots between content, user behavior and outside threats
- Manage insider threats and prevent data loss at the endpoint
- Protect confidential data while your employees are on the web
- Reduce workload with AI-powered data classification

Intelligent Compliance

Data-retention needs are exploding as organizations create more data on more communications platforms. Manage risk with a modern compliance and archiving solution for IT and legal teams. Our cloud-based, people-centric approach helps you:

- Capture and monitor data effortlessly
- Equip your team to scale and manage data growth
- Ease e-discovery and streamline review with machine-learning-assisted automation
- Simplify SEC, FINRA and IIROC compliance
- Ensure compliance on employee social media channels

Get in touch

To find out more about our platform approach to protecting people and defending data, please get in touch with your Account Manager or use our online form to contact us.

Contact us
proofpoint.com/us/contact

USEFUL CONTACT DETAILS

If you would like to contribute to a future issue of New Perimeters, or to give feedback, contact: info@proofpoint.com

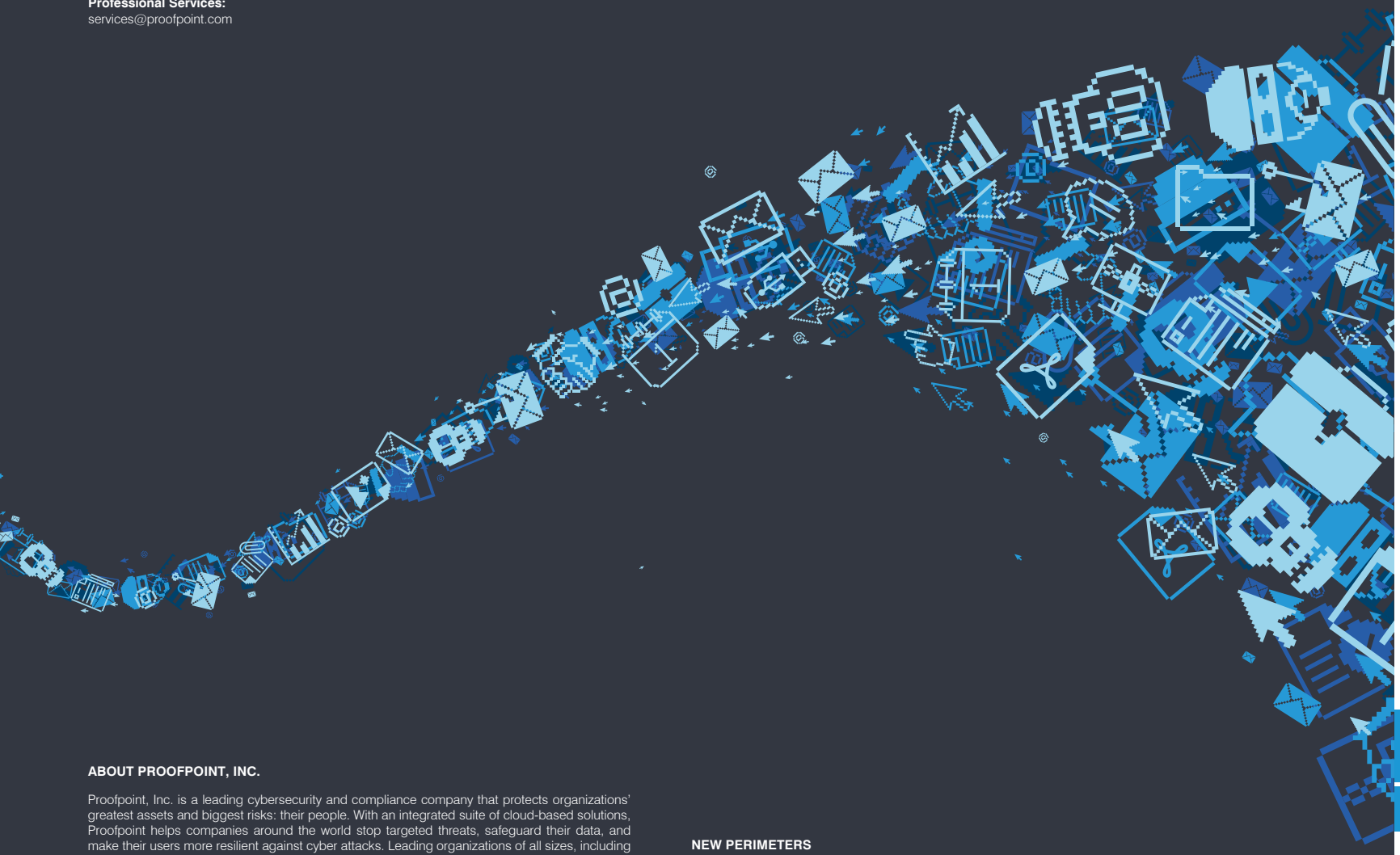
To view the digital version of New Perimeters, visit:
https://go.proofpoint.com/New-Perimeters.html

Technical Training:
www.proofpoint.com/us/support/technical-training
training@proofpoint.com

Proofpoint University:
www.proofpointlevelup.com

Proofpoint Community Support:
www.proofpoint.com/community

Professional Services:
services@proofpoint.com



ABOUT PROOFPOINT, INC.

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including 75 percent of the Fortune 100, rely on Proofpoint for people-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web. More information is available at www.proofpoint.com.

NEW PERIMETERS

This magazine is provided as a statement of direction regarding our product development activities and is provided for discussion purposes only. It should not be relied upon in making a purchasing decision. The development, release and timing of any features or functionality for our products remains at Proofpoint's sole discretion.

proofpoint.