NEW PERIMETERS

MITIGATING RISK THROUGH DIGITAL CHANGE

Threat Spotlight
New Infrastructure, New Risks

Customer Spotlight
Industrial Engineering Leader Fives Aims to Protect Data

Point of View
The Modern CISO’s Guide to Information Protection
CONTENTS

NEW PERIMETERS

CUSTOMER SPOTLIGHT

P30 Industrial Engineering Leader Fives Aims to Protect Data

THREAT SPOTLIGHT

P4 The eight biggest and boldest supplier-linked breaches
P10 New Infrastructure, New Risks
P15 Threat landscape update
P21 Attackers use COVID-19 vaccine lures to spread malware, phishing and BEC
P25 Why OneDrive and SharePoint attacks are successful and how to fight back...

POINT OF VIEW

P34 CISO’s Security Communications Guide
P38 Modern CISO’s Guide to Information Protection
P42 98% of organizations received email threats from suppliers: What you should know
P45 Compliance in the age of digital collaboration
P48 Brief History of Data
P54 Chaos to Efficiency: Migrating from Legacy on-premises Archiving and Compliance Solutions
P57 Top Tips for Remote Work Security: Don’t make it easy for Cybercriminals

Magazine Contributors

Kelig Dugue
Director of Cybersecurity, Fives

Martin Mackay
SVP EMEA, Proofpoint

Vincent Merlin
VP Marketing APJ & EMEA, Proofpoint

Adenike Cosgrove
Director, International Product Marketing, Proofpoint

Maggie Fonseca
Director, Global Programs, Insider Threat Management, Proofpoint

Richard Davis
Group Product Marketing Manager, Proofpoint

Matt Cooke
Senior Product Marketing Manager, Proofpoint

Amanda Anderson
Managing Editor, Proofpoint

Shawn Aquino
Senior Product Marketing Manager, Proofpoint

Rebecca Cleveland
Senior Customer Marketing Manager, Proofpoint

Cover illustration
Peter Henderson - Folio Art

Graphic Design
Chris Cooling - Broadgate Creative
Hello and welcome once again to New Perimeters. In this, our second edition, we are delving into an issue that has the full attention of the C-suite and beyond: digital transformation (DX).

DX is at the heart of every business decision, as organisations look to launch new business models to drive revenue; adapt to new ways of working; build collaboration across the entire supply chain; use technology to change their customer relationships; and innovate for competitive advantage. It is a prerequisite for success, for both B2B and B2C companies.

However, many still overlook the crucial role of the optimized cybersecurity posture as a key enabler of the DX strategy. The critical point is that the technology vendors offering to drive your DX may not give you the necessary strategic protection. And, as recently covered by CSO Online, cybersecurity must take centre stage when mapping your DX journey. The reason is simple: the success of any DX strategy is based on trust. Your customers must trust in your products and services to deliver on their promise and trust that you can keep their data and identity safe from harm.

As DX evolves at pace, bringing with it new levels of efficiency, agility, and responsiveness, it also exposes new points of attack and creates new vulnerabilities.

For every incredible new software-as-a-service (SaaS) offering you launch, a new type of malware emerges to target your data. For every new digital platform you use to enhance customer experience, a new wave of impostors arrives to compromise and defraud your users, and for every new cloud application you embed into your customer journey, a supplier is compromised, putting your data at risk.

Of course, the subject is more topical than ever as you become increasingly reliant on virtual and cloud environments. Gartner reports that 82% of company leaders intend to permit remote working some of the time, with nearly half (47%) intending to allow full-time remote work going forward.

Cybercriminals are already capitalising on the expanding attack surface offered by mass remote work. Attacks are increasingly targeting people. And with more of us accessing data via cloud applications, would-be attackers are presented with multiple new points of attack.

A recent Ponemon report perfectly encapsulated the importance of cybersecurity to digital transformation, covering the steps required to stay safe. But it’s worth pointing out that the role of cybersecurity is not just to stop attacks and limit exposure.

It is also an enabler of change. Effective cyber strategy empowers organisations to improve experiences for employees, customers, business partners and more. By compromising on security, you don’t just put your data at risk. You put the future aspirations and competitiveness of your business at risk too.

As a Proofpoint customer, you are already taking the necessary steps to protect your users as you transform digitally. I invite you to use this publication as a starting point for further discussion.

As always, our Proofpoint team remain on hand to show you how our trusted, people-centric approach can expedite and secure your DX efforts.

If you’d like to start a conversation, or have any feedback on this month’s issue, get in touch at mmackay@proofpoint.com.

Martin Mackay
SVP EMEA - Proofpoint
The eight biggest and boldest supplier-linked breaches

You click an email from your supplier about a delay. You follow the link, log into the portal, and see no shipment information. Assuming a mistake, you get back to your busy day.

Six months later, you suffer a data breach. The authorities trace it back to the email. You’re the victim of a supply chain attack. It’s every company’s nightmare. And for too many, a reality.
Learning that you’ve suffered a cyber attack is one thing but finding out that your supply chain has been weaponised against you is harder to take. When up against such convincing lures, it’s impossible to know who to trust.

Unfortunately, this threat is becoming increasingly commonplace. Half of all cyber attacks now target supply chains. And organisations are under attack from all directions. Last year’s Verizon Data Breach Investigations Report found that 24% of breaches in 2020 involved cloud assets while 40% originated from web apps.

Third-party vendors present a real and growing threat to our organisations. But what can we do to stay prepared?

On the following pages, we look at the biggest, boldest, and most brazen supplier attacks reported in recent years. Every successful attack is an opportunity to learn. When we understand the what, why, and how of supply chain attacks, we can further bolster our defences and strengthen processes with our suppliers.
Attack on IT services supplier exposes frequent flyer data

Year: 2021
Supplier: SITA
Victim(s): Global airlines

IT services operator SITA suffered a “highly sophisticated attack” that potentially exposed Personally Identifiable Information (PII) of hundreds of thousands of individuals. As SITA provides services to 90% of the world’s airlines, the incident had far-reaching implications for the aviation industry.

What do we know?
- Little is known about the methods of the cybercriminals involved. SITA said only that it had been the “victim of a cyberattack”.
- Malaysia Airlines, Singapore Airlines, Finnair, Lufthansa, Cathay Pacific, Air New Zealand, and Air China were among those impacted by the breach.

Cybercriminals lay in wait for months before inserting malicious code

Year: 2020
Supplier: SolarWinds
Victim(s): Microsoft, FireEye, Mimecast, NASA, Malwarebytes, The Pentagon, Intelligence Agencies, Fortune 500 Companies, and thousands more organisations across the globe.

IT vendor SolarWinds suffered a devastating data breach after cybercriminals spent months inside the company’s Orion software and Microsoft Office 365 email system. Malicious code was inserted into software updates which SolarWinds subsequently shipped to thousands of its customers.

What do we know?
- Attackers accessed the vendor’s email system and development environment.
- A malicious ‘Sunburst’ backdoor was injected into an Orion software update.
- The software update was deployed to customers leading to mass infections.
- Further attacks on Orion customers followed once access was established.
- Attacker impersonated internal users at the compromised companies.
Compromised Microsoft authentication certificate puts account credentials at risk

Year: 2021
Supplier: Mimecast
Victim(s): Approximately 10% of Mimecast customers

The Russian hacking group behind the 2020 SolarWinds attack compromised a Microsoft Office 365 Exchange Web Services authentication certificate to exfiltrate encrypted account credentials of Mimecast customers.

The breach affected Mimecast Sync and Recover, Continuity Monitor, and IEP (Internal Email Protect) products.

What do we know?
- Criminal group UNC2452 compromised a Microsoft Office 365 Exchange Web Services authentication certificate.
- Criminals impersonated Mimecast to access encrypted service account credentials.
- Credentials were used to establish connections from Mimecast tenants to on-premises and cloud services, including LDAP, Azure Active Directory, Exchange Web Services, POP3 journaling, and SMTP-authenticated delivery routes.

Ransomware infection at IT supplier puts NASA data at risk

Year: 2020
Supplier: Digital Management Inc. (DMI)
Victim(s): NASA.

Operators of the DoppelPaymer ransomware successfully infected the network of Digital Management Inc. (DMI), a provider of IT and cybersecurity services to NASA, several government agencies, and a number of Fortune 100 companies.

While it is unclear how much data was exposed, the group was able to access NASA-related files and post them on the Dark Web.

What do we know?
- DMI refused to comment on how much of its network was breached.
- The criminal group claimed to have accessed 2,583 servers and workstations, some of which included NASA-related data.
**Compromised employee credentials open the door to a trove of customer data**

Year: 2020  
Supplier: Guest Services Software  
Victim(s): Marriott  

Cybercriminals compromised third-party software to steal the credentials of two Marriott hotel employees and gain access to 5.2 million customer records.  
The exposed data included full names, addresses, phone numbers, and dates of birth.  

**What do we know?**  
- Attackers obtained login credentials of two Marriott employees.  
- Cybercriminals gained access through software used to provide guest services.  
- The network of another unspecified hotel chain was also accessed.

**HR vendor compromise exposes customer bank details**

Year: 2020  
Supplier: Canon Business Process Services  
Victim(s): General Electric  

Cybercriminals compromised an internal email account at Canon Business Process Services, gaining access to General Electric (GE)-related documents.  
The exposed data resulting from the breach impacted GE employees (current and former) as well as many of its beneficiaries.  

**What do we know?**  
- An unauthorised party compromised the email account of the vendor.  
- The account contained substantial personal data, including bank account numbers, social security numbers, passport numbers, and birth, death, and marriage certificates.

**Ransomware attack at manufacturing contractor exposes sensitive data**

Year: 2020  
Supplier: Visser Precision  
Victim(s): SpaceX, Tesla, Boeing, and Lockheed Martin  

A ransomware infection at US manufacturing and design contractor Visser Precision exposed NDAs, billing and payment forms, and military designs. Documents were posted online, with some available to download.  
The breach impacted several big names in aerospace, including Space X, Boeing, and Lockheed Martin.  

**What do we know?**  
- Security researchers report that the attack was caused by the DoppelPaymer ransomware gang.  
- Cybercriminals infected Visser Precision’s PCs and encrypted its files.  
- After infection, files were siphoned from internal networks.  
- When the company failed to pay the ransom by their March deadline, the gang uploaded and exposed a selection of sensitive documents.
Multi-supplier attack exposes Airbus employee data

Year: 2019
Suppliers: Rolls Royce, Expleo, and more
Victim(s): Airbus

Aerospace giant Airbus suffered a series of data breaches after cybercriminals infiltrated its supply chain at several points. In search of commercial secrets, hackers compromised accounts at engine manufacturer Rolls-Royce, technology consultancy Expleo, and two more unnamed Airbus contractors.

What do we know?
- Cybercriminals gained remote access to Airbus via virtual private networks (VPNs) of suppliers.
- Networks of several suppliers were breached long before discovery.
- With suspected links to Chinese nation-state hacking, the group appeared interested in Airbus component certification documents.

Any defence capable of keeping out a threat as convincing and unassuming as supply chain fraud must combine people, process, and technical protections.

This starts by understanding your supplier network. You need to know precisely who holds or has access to your data. From here, you can risk assess and vet the security of each one. This is not a one-time task. Organisations must regularly monitor third-party permissions and network access.

Once you understand who has access, use a Cloud Access Security Broker (CASB) to manage your network, alerting you to unusual requests and other suspicious activity. Advanced email protection and domain authentication is also a must for you and your suppliers to ensure that your suppliers really are who they say they are in email.

Finally, you need to protect your people. All users must know how to detect, deter, and report potential supply chain attacks. They must also understand how their behaviours – credential reuse, unauthorised use etc. – can put your organisation at greater risk.
NEW INFRASTRUCTURE, NEW RISKS
WHY CYBERSECURITY MUST SIT AT THE HEART OF DIGITAL TRANSFORMATION

Digital transformation has been behind every critical organisational decision for some time now. In recent years, however, efforts have increased at pace.

By 2022, 70% of all organisations will accelerate the use of digital technology to transform business practices.¹

By 2025, 75% of business leaders are expected to have leveraged digital ecosystems to expand capabilities and drive into new markets.²

Almost two-thirds of CEOs are accelerating digital business transformation as a result of the pandemic.³

What drove digital transformation in your company?⁴

<table>
<thead>
<tr>
<th>The CEO (6%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The CTO (6%)</td>
</tr>
<tr>
<td>COVID-19 (88%)</td>
</tr>
</tbody>
</table>

Despite the host of benefits on offer, there is a far less positive factor behind the recent acceleration of transformation efforts... COVID-19.

---

¹ - https://www.idc.com/getdoc.jsp?containerId=prUS46967420
² - https://www.idc.com/getdoc.jsp?containerId=prUS46967420
⁴ - Linkedin poll 05.02.2021 - 12.02.2021 / 375 participants
Digital transformation is changing the way we work

**It’s empowering workers**

- 83% of employers believe the shift to remote work has been successful for their company⁵
- 53% of remote workers reported they were likely to work overtime⁶
- 86% of UK CEOs believe the shift towards remote collaboration will endure (78% globally)⁷

**What tools are workers using?**

- 84% of remote workers communicate via instant messaging⁸
- 81% use email
- 76% meet over video
- 54% talk over phone calls

---

⁷ https://www.pwc.co.uk/ceo-survey/ceo-panel-survey.html
⁸ https://hive.com/blog/remote-work-survey-2020-hive/
New infrastructure, new risks

Today’s attacks target people, not just technology.

Cybercriminals are wasting little time capitalising on larger and poorly secured attack surfaces.

If your people are working in unfamiliar environments without adequate training, your organisation is at risk.

Two-thirds of CISOs believe that remote working has made their organisations more vulnerable to attack.

(Source: Proofpoint Global CISO report)

Email fraud risks

Highly targeted email attacks use social engineering rather than technology to exploit human nature. Cybercriminals are opportunistic, using all kinds of subject lines to grab attention.

Popular subject lines:

- Payment 24%
- Request 18%
- Urgent 13%
- Greeting 8%

Insider threat risks

Whether malicious or negligent, the frequency and financial consequences of insider threats have increased significantly in recent years. Between 2018 and 2020:

- Insider threat incidents increased 47%
- The cost of insider threats increased 31% - from $8.76m to $11.45m

Cloud and shadow IT risks

With mass remote working here to stay, businesses will increasingly rely on remote cloud environments.

- 44% of IT leaders believe this explosion of cloud usage will be one of the biggest cybersecurity threats to mitigate in the next two years
- 43% believe the biggest threat will be the rise of shadow IT or unmanaged data storage due to the increased remote workforce.
- Only 8% of companies know the scope of shadow IT at their organisations

11 - https://www.proofpoint.com/sites/default/files/white-papers/UK_CISO-REPORT_FINAL.pdf
Cybersecurity tops investment priorities for the next 12 months across all maturity levels

Share of respondents citing each area as a ‘very high priority’ for investment over the next 12 months, by digital maturity level.13

<table>
<thead>
<tr>
<th>Area</th>
<th>A - LOWER MATURITY</th>
<th>B - MEDIUM MATURITY</th>
<th>C - HIGHER MATURITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBERSECURITY</td>
<td>46%</td>
<td>53%</td>
<td>67%</td>
</tr>
<tr>
<td>CLOUD</td>
<td>26%</td>
<td>44%</td>
<td>59%</td>
</tr>
<tr>
<td>DATA ANALYTICS</td>
<td>27%</td>
<td>43%</td>
<td>57%</td>
</tr>
<tr>
<td>DIGITAL BUSINESS MODELS</td>
<td>22%</td>
<td>39%</td>
<td>57%</td>
</tr>
<tr>
<td>PROCESS AUTOMATION</td>
<td>22%</td>
<td>39%</td>
<td>57%</td>
</tr>
<tr>
<td>DIGITAL SAVVY</td>
<td>23%</td>
<td>40%</td>
<td>54%</td>
</tr>
<tr>
<td>UNIFIED CUSTOMER EXPERIENCE</td>
<td>21%</td>
<td>39%</td>
<td>55%</td>
</tr>
<tr>
<td>DEVOPS</td>
<td>21%</td>
<td>35%</td>
<td>49%</td>
</tr>
<tr>
<td>OPEN NETWORKS</td>
<td>19%</td>
<td>36%</td>
<td>46%</td>
</tr>
<tr>
<td>ECOSYSTEM</td>
<td>16%</td>
<td>35%</td>
<td>50%</td>
</tr>
</tbody>
</table>


A new approach

Digital transformation is changing the way we do business. More than ever, your success hinges on the strength and reliability of your connections – between your workers, with your business partners, and to your customers.

This creates new security, compliance, and fraud risks far beyond the scope of network-focused defences. That’s why digital transformation calls for a new approach.

As your business transforms, so does your risk profile. And your cyber strategy must transform with it – to secure new attack points, train users in new environments, and ensure your digital ambitions are not putting your organisation at risk.
THREAT SPOTLIGHT

THREAT LANDSCAPE UPDATE

IN TODAY’S THREAT LANDSCAPE, PEOPLE ARE THE NEW PERIMETER. WHETHER IT’S MALWARE, EMAIL FRAUD, CLOUD ACCOUNT TAKEOVER OR CREDENTIAL PHISHING, CYBER ATTACKS NO LONGER FOCUS ON BREAKING THROUGH NETWORK CONTROLS AND CRACKING TECHNICAL FLAWS. INSTEAD, THEY TARGET USERS AND EXPLOIT HUMAN NATURE.

That’s why people are at the centre of our cybersecurity mission – and why user-activated attacks are the focus of this report. Like most threat reports, this one highlights the latest quarter’s attack trends, campaigns and themes. But it goes a step further, exploring how attackers target people and what you can do about it.

Our goal in this report is twofold. First, we want to help demystify cybersecurity by shedding light on the people-centric nature of today’s threats. Second, and just as critical, we want to show how organizations can use this insight to better protect their greatest asset and today’s biggest risk: their people.

The report is a small slice of the insight we offer customers through the Proofpoint Nexus Threat Graph. Every day, we analyze billions of email messages, billions of URLs and attachments, tens of millions of cloud accounts and more – trillions of data points across all the digital channels that matter. Our global footprint and laser focus on people-related cyber risk give us a unique view into today’s biggest cyber threats.

Except where noted, this report covers threats observed directly by our global network of threat researchers.

Top attack techniques

Email is by far the most used channel for cyber attacks of 2020. We saw a wide range of email attack techniques in the fourth quarter, but almost all of them included some form of social engineering.

The term “social engineering” can include any number of psychological techniques that trick people into doing something the attacker wants them to do. That may mean opening an attachment, clicking on an unsafe URL, sending login credentials or sensitive information or even wiring money to the attacker.
Figure 1, below, shows attacks that used social engineering in tandem with a technical exploit or technique. In many cases, social engineering is used to trick users into doing something directly – no malware needed. If listed as a separate technique, social engineering would easily dominate the chart as a component in 99% of all attacks.

When used with a technical exploit, social engineering might be something as simple as creating a hard-to-resist subject line and spoofed email address. In other cases, it might be as involved as impersonating a trusted colleague to lure new victims.

Here’s a summary of the most common techniques:

- **Office macros**: Exploits flaws in a mini-programming language designed to help automate and extend Microsoft Office features. Attackers use it to create and embed malicious macros that infect users’ devices when opened. Most attacks involve tricking the user into not just opening the document but enabling macros. Many recent attacks feature a new twist on a decades-old feature of Excel. These are often classified as Excel 4.0 (XL4) attacks.

- **Sandbox evasion**: Modern threat-detection tools safely “detonate” unknown files within virtual machine settings to see what they do when clicked or opened. Sandbox evasion techniques can prevent the malware from running or limit telltale behaviors in virtual environments to avoid being discovered. One of the big evasion techniques we saw in Q4 was using Windows’ Regsvr32 command line tool in a way that is not detected within most sandboxes. (Regsvr32 was designed to help PC administrators, but it can be exploited to let attackers bypass Windows’ AppLocker security tool.)

- **PowerShell**: Exploits Windows’ built-in administration tool to infect victim’s PCs. These attacks usually start with a phishing email that includes a URL that links to a page with embedded code that uses the PowerShell feature to take over the victim’s machine. These attacks are hard to detect because they use a legitimate Windows feature and don’t start with a full malware file. The feature can also be used to download and run other malicious files from the internet.

- **HTML**: Web pages can include all kinds of code that exploits flaws in popular browsers and, on rare occasions, operating systems. These include legitimate but compromised websites and web-based ads. Most attacks that use this technique trick the victim into clicking an unsafe URL, but attackers can also send HTML pages directly through email.

- **Thread hijacking**: After taking over someone’s email account, the attacker contacts people the compromised user knows, replying to past and ongoing email threads with a malicious email.

- **Password protected**: Adding password protection to a malicious file can lock it away from many malware-detection tools. The attacker gives human readers the password and tricks them into opening and unlocking the file.

- **Geofencing**: Limits malware behaviors to defined geographies using the infected device’s GPS and other location features. This technique is used to target attacks or evade detection tools.
Top Threat Actors

Among malicious emails we could tie to a known threat actor, more than 60% of the total volume we saw in Q4 came from just two attackers, which we have designated as TA544 and TA542 (also known as Emotet). Both attackers were also among the most prolific threat actors in Q3.

Note: This charts highlights email attacks that we could confidently tie to a known threat actor. Determining who is behind an attack, a process known as attribution, is not always possible. The cyber criminal ecosystem is vast and highly fragmented. Unattributed attacks are not included in this chart to analyze and compare the biggest threats.

What are ‘Threat Actors?’

Threat actors is a term threat researchers use to describe an attacker or groups of attackers. They can include:

- **State-sponsored attackers.** Also known as advanced persistent threats (APTs), these attackers typically engage in espionage on behalf of a government. But attackers may also involve intellectual property theft, outright financial theft and attacks designed to disrupt or damage data and systems. Whatever approach they take, they’re all meant to achieve a military or diplomatic goal.

- **Cybercriminal rings.** These organized crime groups are usually in it for the money. In many cases, they work like multilevel marketing franchises. An advanced threat actor creates the malware “product” and sets up the infrastructure as an easy-to-use package or service. Lower-level cyber criminals may rent the service for their attacks, paying to use it for a set period of time or getting a cut for each successful compromise. In other cases, they act as distributors, sending out emails with the malware and earning a commission on each successful infection. Some researchers consider the most advanced cybercriminal groups to be APTs.

- **Hacktivists.** This portmanteau of “hacking” and “activism” refers to attacks meant to make a political statement or effect policy change. These attacks, though rare, typically expose secret information, disrupt perceived wrongdoing or embarrass foes. While their goals are different, they use many of the same tools and techniques as other types of attackers and can cause just as much harm.

Knowing who is behind an attack – and what their motivations are – can be a critical part of defending against them.
TA542 and the demise of Emotet

TA542 has become one of the most prolific in recent years due to massive campaigns that use a malware strain called Emotet. The group has targeted multiple industries around the world, sending hundreds of thousands – or even millions – of messages per day.

Dubbed “the world’s most dangerous malware,” Emotet is versatile and highly adaptable. It was first discovered in 2014 as a simple banking Trojan aimed at stealing account credentials. Since then, it has evolved into a highly versatile malware strain used for everything from stealing data to harvesting email to ransomware. Emotet has been used to target critical industries around the world, including banking, e-commerce, healthcare, academia, government and technology.

Emotet doesn’t just compromise the systems it infects. It also uses these compromised machines to launch new attacks, absorbing them to a zombie-like network of more than a million similarly infected machines known as a botnet. Other cyber criminals can pay TA542 to use the botnet for all kinds of attacks – or could until just a few weeks ago.

The takedown

Authorities said in late January that they had shut down Emotet’s infrastructure as part of a coordinated effort across nine countries in North America and Europe. Law enforcement appears to have taken over all three of Emotet’s known botnet networks. Authorities plan to retool the botnets to remove its own malware from infected systems.

What’s next?

At this stage, there’s no telling what Emotet takedown means over the long term. TA542 had remained active in the days leading up to the shutdown, and efforts to disrupt large botnets in the past have had mixed results.

We don’t know how large the team was operating the Emotet botnet and whether all of its members were in the Ukraine, where at least two of Emotet’s operators were arrested.

If segments of the botnet and associated operators survive, Emotet’s source code may be retooled under a new infrastructure and new moniker. Threat actors often build redundancy into their infrastructure, and their teams often live in countries beyond the reach of the law.

TA544 goes on a financial cyber crime spree

First documented in 2017, TA544 is part of a financial crime ring that has targeted a range of industries in Japan and several European countries, with a heavy focus on manufacturing and tech firms. It is an affiliate that distributes several strains of malware, including Panda Banker and others.

A large share of its attacks use a Trojan called Ursnif, but it’s not clear whether it controls Ursnif or is just one of the groups using it. The malware stems from leaked source code and is used by many other threat actors. One of TA544’s distinctive traits is how it uses steganography, hiding malicious code in seemingly benign images.

TA573: a top-tier distributor with ties to Evil Corp

Like other illicit markets, cyber crime is a loose, multilayered ecosystem that includes suppliers, distributors, money launderers and other specialties. TA573 operates as a malware “affiliate”, which sends malware someone else has created.

Think of affiliates as the last mile of the malware supply chain. They don’t write malware or run the infrastructure used to support attacks. Instead, they’re the malware distributor, selecting targets and crafting emails designed to trick recipients into engaging with them. Cyber criminals’ business models vary, but affiliates typically get a commission on every victim infected.
TA573 is an affiliate distributor of Dridex, a malware strain that resurged in 2020 after a lying low through most of 2019. The malware itself is a creation of a Russian cyber crime group that calls itself Evil Corp, a longtime menace that recently turned to ransomware. In June, U.S. authorities offered $5 million for information leading to the arrest of Evil Corp’s operators, the largest reward ever for a cyber criminal.

**TA800 holds healthcare data hostage**

This attacker is an affiliate distributor of the The Trick, also known as Trickbot, and BazaLoader. (For more on how affiliates work, see the description of TA573).

TA800 has targeted a wide range of industries in North America, infecting victims with banking Trojans and malware loaders (malware designed to download other malware onto a compromised device). Malicious emails have often included recipients’ names, titles and employers along with phishing pages designed to look like the targeted company. Lures have included hard-to-resist subjects such as related to payment, meetings, termination, bonuses and complaints in the subject line or body of the email.

In Q4, it was responsible for a wave of attacks against the healthcare sector using a loader called BazaLoader. BazaLoader, under the control of a separate threat actor, subsequently installed a ransomware strain called Ryuk. (Some researchers believe BazaLoader was created by the same malware team behind The Trick – in part because both malware strains infected victims with Ryuk).

Ransomware encrypts data on infected devices, effectively locking victims out of their data and systems until they pay the attacker to regain access.

Healthcare organizations have become an especially enticing target for ransomware attacks. They are often not as well protected as other sectors and the life-and-death nature of the business means they can afford little downtime.

Three U.S. government agencies warned hospitals in October of an “increased and imminent” cyber crime threat that included ransomware attacks.

**TA574: a new entrant draws on legacy malware**

A relative newcomer, TA574 appears to be another affiliate focused on malware distribution. (For more on how affiliates work, see the description of TA573).

TA574 has launched attacks against a wide range of industries, sending an updated version of a 15-year-old banking Trojan called Zloader. It’s an offshoot of the infamous Zeus banking Trojan, which has been used to steal millions of dollars from victims’ banking accounts.

The group also uses Ostap, a malware downloader that uses JavaScript to hide itself from security sandbox analysis tools (see the “Top Attack Techniques” section for more on sandbox evasion).
Attribution: the known unknowns

As noted earlier in this section, Figure 1 includes only attacks that can be tied to a known threat actor. This focus is helpful but may make the universe of attackers seem more concentrated than it actually is.

As Figure 2 (below) shows, nearly 90% of campaign-related email volume we saw in Q4 can’t be attributed to known attackers. (That figure is even higher for email that is not part of a campaign).

Conclusion and recommendations

Today’s attacks target people, not infrastructure. That’s why you must take a people-centric approach to cybersecurity. That includes user-level visibility into vulnerability, attacks and privilege and tailored controls that account for individual user risk.

Here’s what we recommend as a starting point.

- Train users to spot and report malicious email. Regular training and simulated attacks can stop many attacks and help identify people who are especially vulnerable. The best simulations mimic real-world attack techniques. Look for solutions that tie into real-world attack trends and the latest threat intelligence.

- At the same time, assume that users will eventually click some threats. Attackers will always find new ways to exploit human nature. Find a solution that spots and blocks inbound email threats targeting employees before they reach the inbox. Invest in a solution can manage the entire spectrum of email threats, not just malware-based threats. Some threats – including business email compromise (BEC) and other forms of email fraud – can be hard to detect with conventional security tools. Your solution should analyze both external and internal email – attackers may use compromised accounts to trick users within the same organization. Web isolation can be a critical safeguard for unknowns and risky URLs.

- Manage access to sensitive data and insider threats. A cloud access security broker can help secure cloud accounts and help you grant the right levels of access to users and third-party add-on apps based on the risk factors that matter to you. Insider risk management platforms can help protect against insider threats, including users compromised by external attacks.

- Partner with a threat intelligence vendor. Focused, targeted attacks call for advanced threat intelligence. Leverage a solution that combines static and dynamic techniques at scale to detect new attack tools, tactics, and targets – and then learns from them.

Attribution: the known unknowns

As noted earlier in this section, Figure 1 includes only attacks that can be tied to a known threat actor. This focus is helpful but may make the universe of attackers seem more concentrated than it actually is.

As Figure 2 (below) shows, nearly 90% of campaign-related email volume we saw in Q4 can’t be attributed to known attackers. (That figure is even higher for email that is not part of a campaign).

It’s easy to see why. Would-be hackers with little technical skill can easily access the malware and infrastructure they need for successful campaigns, greatly lowering barriers to entry. And as explained in the previous section, many attacks don’t require these tools at all – just a keen understanding of human nature and a knack for persuasion.

It’s a testament to the breadth and diversity of today’s threat landscape – and a reminder that organizations looking to protect their users, data and systems must be prepared for anything.

3. Danny Palmer (ZDNet). “Emotet: The world’s most dangerous malware botnet was just disrupted by a major police operation.” January 2021.
Attackers use COVID-19 vaccine lures to spread malware, phishing, and BEC

Proofpoint has observed the use of COVID-19 in broad-scale social engineering attacks leading to malware, credential phishing, and BEC since the beginning of the pandemic. We have observed COVID-19 themes consistent with current events throughout this healthcare crisis. Initially, we saw lures around the virus’s existence, which then turned to ancillary lures such as medical supply shortages.

As anticipated, over the last two months, Proofpoint researchers observed more attacks that leverage the COVID-19 vaccine news, such as approvals of the vaccine by world governments, logistics of vaccine deployment, and distribution of the vaccine to frontline responders and other individuals.

In this article, we provide examples of email-borne attacks spreading malware, phishing, and BEC. These examples exemplify abuse of popular brands such as WHO, DHL, and vaccine manufacturers delivered to users in organizations located in the United States, Canada, Austria, and Germany. The lure themes leveraged a range of topics, including fear that a person had encountered an infected individual; government vaccine approvals and economic recovery fuelled by the vaccine; as well as sign up forms to receive the vaccine, information updates, and vaccine shipment delivery.
“COVID Vaccine Anticipation Merger and Acquisition” BEC

I hope all is well with you.
The world economy is approaching a turning point amid hopes for a rapid recovery fuelled by an early vaccine, despite renewed lockdowns worldwide. We must now position ourselves for the impending economic upturn even as we maintain vigilance in this uncertain period.
In the midst of every crisis lies great opportunity. I am excited to share that after much careful consideration, we have decided to acquire the assets of a distressed foreign company. Our legal team is currently working on closing the transaction and I need you to work with them on certain time-sensitive issues.
We have named this acquisition “Project Yeti” and I need to count on your discretion in this very confidential matter.
Please let me know when you are available and the best number to reach you at.
Regards,

Date: Mon 12/7/2020 7:26 AM
From: ••••••••••••••••
Subject: Project Yeti

Figure 1: A malicious email purporting to be from an executive and asking the recipient for their cooperation in a confidential acquisition.

From December 1 to December 15, 2020, Proofpoint observed a large BEC campaign (thousands of emails) spoofing executives and attempting to elicit the recipient’s support in a bogus merger and/or acquisition. These emails targeted various personnel in roles such as Vice President, General Manager, and Managing Director. The emails were primarily sent to companies in the United States.

These emails projected that COVID-19 vaccines would fuel the world’s economic recovery. The email purported to be from an executive asking the recipient for their cooperation in a confidential acquisition of a foreign company. It claimed that this is an opportune moment to make the acquisition as in the “midst of every crisis lies a great opportunity.”

Office 365 Phishing

Date: Fri, January 1, 2021 at 7:56 AM
From: ••••••••••••••••
Subject: 40 Million COVID-19 Vaccine Dose Supply

Government approves Covid-19 vaccine as it moves to inoculate tens of millions.
Confirm your email to be enlisted to receive vaccine.

https://•••••••••••••.online

Figure 2: The malicious email with an Office 365 phishing URL.

Figure 3: Phishing landing page with a red button asking users to “Login with office 365”.

In this medium-sized campaign (hundreds of messages), threat actors began delivering messages on January 1, 2021, over four days, targeting dozens of different industries in United States and Canada. The emails urged the potential victims to click a link to “confirm their email to receive the vaccine”. The goal of this phishing campaign was to steal Office 365 login credentials (email and password).

This campaign was notable because it capitalized on the recent government approval of vaccines and the rush to receive it. Specifically, the email talks about “Government approval of the COVID-19 vaccine” and provides a link where one can supposedly
register to receive it. At the time of this campaign, the vaccine in the United States was only available to first responders and doctors on the front lines.

The campaign also abused the brands of COVID-19 vaccine manufacturers as the lure in some of the emails. Other emails did not mention specific brands.

Example subjects included:
- [Vaccine manufacturer] COVID_19 Vaccine
- 40 Million COVID-19 Vaccine Dose Supply
- COVID-19 Vaccine

**“Complete a task for me, before I leave for a COVID-19 vaccine meeting” BEC**

Fig. 4: The malicious email asking the recipient for their personal information.

On January 11, Proofpoint researchers observed another small (under 100 emails) BEC email campaign. The emails targeted various industries in the United States.

This campaign is another excellent example of BEC actors picking vaccine lures in an attempt to exploit their targets. This specific email only mentions the COVID-19 vaccine meeting in passing; however, it adds urgency – a common BEC technique – to the follow-up request: “Please give me your personal number?”. This attempts to increase the stress by giving the recipient less time to think about their response and allowing the attacker to pivot outside of a protected ecosystem.

**AgentTesla Malware**

Fig. 5: AgentTesla abuses World Health Organization Brand.

On January 12, 2020, Proofpoint observed a medium-sized (several hundred messages) email campaign targeting many industries in the United States. The email contained an attachment, “DOWNLOAD-NEW VACCINES-COVID-19-REPORT-SAFETY1.xlsx.iso” which included an embedded executable file named “DOWNLOAD-NEW VACCINES-COVID-19-REPORT-SAFETY1.xlsx.exe”. This executable, if run by the user, drops and runs the AgentTesla keylogger.
This campaign is notable due to the subject, “COVID-19 APPROVED NEW VACCINES”, in the email lure and abuse of the World Health Organization logo and name. Additionally, Proofpoint has observed this specific actor spreading RATs, stealers, keyloggers, and downloaders since at least 2019. In March 2020, they used their first COVID-19 email lures, and since then, we have watched them adapt their COVID-19 lures to the current news cycles, to include mentions of the vaccine.

DHL Themed Phishing

Dear •••••••••
You have undelivered package from DHL Office. We are having problem with delivery on your address. Please go online to submit your correct address so we can deliver your package today.

GO ONLINE HERE
With kind regards,
© DHL International GmbH. All rights reserved.

Figure 6: An email purporting to inform the recipient about an undelivered DHL vaccine package.

Figure 7: Phishing landing page with DHL branding asking for user’s username or Email address and password.

On January 14, 2021, Proofpoint researchers observed a medium-sized (hundreds of messages) campaign targeting dozens of different industries in the United States, Germany, and Austria. The emails urged the potential victims to click a link to “go online to submit your correct address so we can deliver your package today”. The goal of this phishing campaign was to steal email login credentials (email address and password).

While the email body content is typical for a package delivery service phish, the notable difference was in one of the subject variants. The subject “COVID-19 vaccine distribution-Re-confirm your delivery address” implied to the recipient that the specific package is supposedly a COVID-19 vaccine.

<table>
<thead>
<tr>
<th>IOC</th>
<th>IOC Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bf78ad88ad9124adde7b3f56f87f5e-848d042ae56acbb75bc7f71962c6a5f68</td>
<td>SHA256</td>
<td>DOWNLOAD-NEW VACCINES-COV-ID-19-REPORT-SAFETY1.xlsx.iso</td>
</tr>
<tr>
<td>2a0b7eba6ec8d395dcc4485e2369c2ec-289819c378e0f1f1a87a7622e0da17c</td>
<td>SHA256</td>
<td>DOWNLOAD-NEW VACCINES-COV-ID-19-REPORT-SAFETY1.xlsx.exe</td>
</tr>
<tr>
<td>hxxp://putrajayagemilani.com/covid_19_vaccine_delivery/dh?lo=[base64 of recipient email]</td>
<td>URL</td>
<td>January 14, 2021 DHL themed phishing link</td>
</tr>
</tbody>
</table>
Why OneDrive and SharePoint attacks are successful and how to fight back...

Threat actors have followed the enterprise migration to the cloud. They compromise and take over user accounts to move laterally inside an organization, steal data, or communicate with your business partners or customers to request fraudulent wire transfers. They use your cloud and email infrastructure to host and distribute malicious content. Attackers leverage your users’ contacts and study their emails to understand trust relationships and map organizations. Exploiting the way modern employees work such as file sharing, attacks can be more effective than ever. In fact, Proofpoint research shows that users are seven times more likely to click on malicious SharePoint Online and OneDrive links that are hosted on legitimate Microsoft domains.

In the first half of 2020, Proofpoint detected 5.9 million email messages with malicious SharePoint Online and OneDrive links. While these messages made up about 1% of the total sample of messages with malicious URLs, they represented more than 13% of user clicks. Users were:

- Four times more likely to click on malicious SharePoint links
- 11 times more likely to click on malicious OneDrive links

We also discovered that these messages were distributed from over 5,500 compromised tenants, which represent a large portion of Microsoft’s enterprise customer base. Such a wide-spread and effective form of cyberattack deserves a closer look.
Malicious SharePoint/OneDrive Links and Account Takeover Lifecycle

SharePoint phishing usually starts with cloud account compromise. Once in control of the account, the attacker uploads a malicious file and then changes the sharing permissions of the file to “Public” so the new anonymous link can be shared with anyone. The attacker emails the link or shares the link with the user’s contacts or other targeted accounts, including external ones. When the recipients open the file and click on the embedded malicious link, they are phished, which starts the whole cycle again. These attacks can lead to data theft or wire fraud such as supply chain fraud.

PDF Example:

In the example below, a user receives an email with a shared link to a pdf file (INV_1100110.pdf) that looks like an invoice. When the user clicks on the link in the pdf file, he is directed to a phishing site that is a fake OneDrive sign-in page.

Sometimes the link in the shared document can be a redirect URL that is unique and hence can be difficult to detect, as it would not appear on any URL reputation repository.

OneNote Example:

Here is an example of an attack that uses SharePoint to host a malicious OneNote file impersonating voice mail:

Malicious OneNote files can also be challenging since they cannot be downloaded and sandboxed. Detection requires an additional step - web-scraping before the embedded links can be analyzed.
Microsoft Form Example

In this example, the cybercriminal shares a Word document with a link to a publicly shared Microsoft Forms file (the fake login page), which he uses to harvest Office 365 credentials. Given this attack utilizes legitimate Microsoft services and is pure social engineering, it poses more of a challenge to detect and even harder to block/mitigate if you lack visibility into both email and cloud environments.

OneDrive Portal

1. USERNAME:*  
   enter your username  
   Enter your answer

2. SIGNIN:*  
   login here to view shared document  
   Enter your answer

Submit

Never give out your password. Report abuse

WE HAVE ALSO OBSERVED SOME ATTACKERS HOSTING MALICIOUS CONTENT IN ONE TENANT WHILE UTILIZING A COMPROMISED ACCOUNT SUCH AS THAT OF A VIP IN A SECOND TENANT.

Sharing the malicious link from the account of a more fitting user would increase the attackers’ chances of success. In addition, even if the compromised account in the second tenant is discovered, the malicious file hosted in the first tenant would not be taken down. And so, the attack would persist.
Top 10: Collaboration services domains with clicked-on malicious links

SharePoint Online and OneDrive are not the only collaboration services domains that are abused by attackers. The graph below shows the top 10 list for such domains by clicks on malicious links hosted on those domains in the first half of the year. A notable one is Sway, the new Microsoft app for creating and sharing interactive content such as reports and newsletters. A second one is storage. Googleapis, which is a file (like a software patch) hosting service that attackers use for tech support scams and more.

<table>
<thead>
<tr>
<th>Domain Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>my.sharepoint.com</td>
<td></td>
</tr>
<tr>
<td>1drv.ms</td>
<td></td>
</tr>
<tr>
<td>onedrive.live.com</td>
<td></td>
</tr>
<tr>
<td>storage.googleapis.com</td>
<td></td>
</tr>
<tr>
<td>docs.google.com</td>
<td></td>
</tr>
<tr>
<td>sway.office.com</td>
<td></td>
</tr>
<tr>
<td><a href="http://www.dropbox.com">www.dropbox.com</a></td>
<td></td>
</tr>
<tr>
<td><a href="http://www.dropbox.com">www.dropbox.com</a></td>
<td></td>
</tr>
<tr>
<td>fibrebasestoarge.googleapis.com</td>
<td></td>
</tr>
<tr>
<td>app.box.com</td>
<td></td>
</tr>
</tbody>
</table>
Defending against Hybrid Email and Cloud Threats

To defend against hybrid attacks like SharePoint and OneDrive phishing, organizations must gain visibility across email and cloud threat vectors and address the attack chain holistically. You need to understand your very attacked people (VAPs) and the risks they pose to your organization:

- Who is being targeted with high-priority threats?
- What techniques are being used to attack users?
- Who has clicked on malicious links?
- Which users are prone to clicking?
- Which accounts are compromised?
- Which compromised accounts show suspicious file activity?

Proofpoint Targeted Attack Protection and CASB bring our people-centric approach to email and cloud security and defend cloud accounts against such attacks using advanced analytics such as:

- Predictive sandboxing of email messages with links from collaboration services such as SharePoint, OneDrive, Google Drive, Dropbox, etc.
- URLs are rewritten to protect users on any device or network as well as provide real-time sandboxing on every click
- Compromised account detection and remediation
- Adaptive access controls that prevent unauthorized logins or enforce multifactor authentication for risky ones
- Post account takeover file and mailbox activity detection and mitigation.

Proofpoint Security Awareness Training delivers targeted education driven by threat intelligence to ensure the right response from your users when faced with sophisticated attacks such as SharePoint and OneDrive phishing.
Industrial Engineering Leader Fives Aims to Protect Data

People Centric Security Helps Control Risk of Data Loss
Fives is an industrial engineering group, headquartered in Paris, France. It designs and manufactures machines, process equipment and production lines for the world’s largest industrial players including steel, aeronautics, aluminium, automotive, cement, energy, logistics, glass and more.

In 2019, Fives achieved a turnover of 1.99 billion euros. And it employed nearly 8,400 people across 80 companies in some 30 countries.

Supporting global industry leaders at every stage of their production cycle requires solutions to prevent identity theft and data loss to protect industrial and intellectual property. As massive ransomware attacks began to hit the world, Fives realized it needed to strengthen the security of its Office 365 messaging system. It also needed to support its employees with security best practices. Attackers use social engineering techniques to get employees to open a fraudulent attachment or click on a malicious link. And there’s a constant evolution of threats in work environments, which includes an increase in malicious URLs.

This has accelerated the organization’s commitment to implement a truly people-centric defense strategy. “The legacy solution we were using to protect our messaging was not working to our satisfaction. Following several peer recommendations, we decided to conduct a proof of concept with Proofpoint to compare the performance of the two solutions,” explains Kélig Dugué, Director of Cybersecurity at Fives.

Increased Visibility

The proof of concept for Proofpoint Cloud App Security Broker (CASB) was decisive. “We quickly realized the full potential of this solution. Its ability to give us visibility into users and data, generate alerts and navigate in analytics dashboards, convinced us. We were particularly fond of its user interface,” explains Kélig Dugué.

“The scale of the 2017 Wannacry and NotPetya ransomware attacks led to a real awareness of cyber risks. Protecting email became a priority for us.”

Kélig Dugué
Director of Cybersecurity, Fives
Tailor made project management

The project gained momentum and took on a new dimension when Fives decided to federate the company’s intranet with Office 365. The transition from an application-based intranet to a collaborative solution, a Digital Workplace, had to be done without compromising security. In fact, it had to improve security while simplifying the user experience by reducing the number of required passwords.

A new proof of concept was then launched with Proofpoint CASB and Ilex Sign&Go. This was to ensure that the authentication environment had the right configuration. Proofpoint was the leader on this project and highlighted its flexibility, responsiveness and ability to quickly deploy its solution in complex environments. It took less than five months to complete the Fives Digital Workplace federation project.

A stronger last line of defense

In addition to its infrastructure protection, it’s a key mission of the Fives security team to support employees in implementing good security practices. Fives recognized that a security-conscious employee can be the last line of defense against an attack. The company deployed Proofpoint Security Awareness Training (PSAT), which simulates phishing attacks and encourages its users to play a key role in identifying and blocking these attacks. Employees can simply click on a button to report suspicious messages. With these comprehensive features, Fives puts people at the heart of its security strategy. This helps to reduce the exposure to threats and effectively protects against attacks.

With Proofpoint, the entire risk management process is optimized. There’s faster identification of potential account compromises, enabling instant, accurate reporting to the monitoring team. They can then make informed decisions quickly, such as changing a password, revoking OAuth tokens and more. And now it only takes a few minutes from detection to neutralization of active threats.

Did you know?

You can protect your users and data with Proofpoint’s people-centric security for cloud apps. Proofpoint Cloud App Security Broker combines compromised account detection, data loss prevention (DLP), cloud and third-party apps governance with adaptive access controls to help you secure Microsoft 365, Google Workspace, Box, Salesforce, AWS, Azure, Slack and more.
THE CHALLENGE

- Protect data and intellectual property against attacks
- Master access management and information sharing in different environments, including Microsoft Office 365
- Support employees with best practices and security solutions

THE SOLUTION

- Proofpoint Email Protection
- Proofpoint Targeted Attack Protection (TAP)
- Proofpoint Threat Response Auto-Pull (TRAP)
- Proofpoint Internal Mail Defense (IMD)
- Proofpoint Cloud App Security Broker (CASB)
- Proofpoint Security Awareness Training (PSAT)

THE RESULTS

- Protected against 95% of phishing attacks and malware infections in Office 365 in one year
- Enhanced visibility into account compromise risks through alerts and analysis dashboards
- Reduced time spent searching for, understanding, and neutralizing active threats
- Controlled costs

WITH PROOFPOINT, THE ENTIRE RISK MANAGEMENT PROCESS IS OPTIMIZED. THERE'S FASTER IDENTIFICATION OF POTENTIAL ACCOUNT COMPROMISES, ENABLING INSTANT, ACCURATE REPORTING TO THE MONITORING TEAM.
Why CISOs must master the art of positive communications

By Andrew Rose
Resident CISO, EMEA - Proofpoint

Though one of the most recent additions to the C-suite, the CISO has taken centre stage in recent years. Such is the high-profile nature of the role that 90% of CISO’s are regularly summoned before the board to make business recommendations.

Despite this greater prominence, it is a role that is rarely afforded equal billing with others in the boardroom. Of the 62% of Fortune 500 companies with a CISO in place, just 4% list the individual responsible on their leadership pages.

This lack of recognition is likely because appointing a CISO was traditionally viewed as a compliance exercise rather than a transformational one. Generally speaking, the CISO is asked to advise when something goes wrong. Be it an internal issue or a headline-hitting data breach elsewhere.

While cybersecurity may once have had a limited remit, that is certainly not the case anymore. As the march toward digital transformation continues at pace, the CISO’s role is not to temper progress with controls, process, and protections but to facilitate it.

More robust and intelligent security means faster, more flexible services and improved employee experiences. Delivering this message and changing the narrative around cybersecurity is not easy. But with clear communication and positive interactions, it is certainly possible. Here’s how.
Setting the tone

Many users view cybersecurity as a dry subject, meaning they’re likely to switch off. To overcome this, structure your communications to make them engaging and accessible.

Include snappy titles to hold the reader’s attention, and break information down into bullets and bitesize chunks.

If you’re sending a particularly long message, start with a summary or TL;DR (Too Long; Didn’t Read.) so users can quickly scan through the important points.

Finally, if you’re warning of a particular lure or scam, use real-world examples to help the reader relate.

Choosing the right channel

The method of communication is just as important as the message. So, it’s vital that you send the right information to the right people via the right channel.

Email is the most common contact method, but it cannot be relied upon when urgent action is required. SMS is a better option in this instance.

Longer form and less time-sensitive information can be shared via intranets and physical noticeboards. Both mediums also work well to reinforce key messages.

As it is viewed as a less formal channel, instant messaging should be avoided when communicating essential updates. However, it can be a helpful way to point users in the direction of other resources.
Timing is everything

Communication fatigue is a very real issue when conveying vital information. When users feel bombarded with information, they are more likely to disengage. Try not to overwhelm users to the point that they start to filter out your messages. Make sure that you only communicate when it is required.

You should also look to weave security messaging in with other communications wherever possible. This can help the reader understand cybersecurity in the context of corporate culture, new technology deployments, and other company updates.

Honning your message

The content of your communication is key. While the when and the how are critical, nothing is more important than the what.

The goal here is to build positive associations with cybersecurity. Instead of issuing orders or demands, educate users on the reasons why they need to take action. Combine both “run toward” and “run away” style messaging to appeal to all personality types.

You also need to ensure that users are empowered to act. Make any instructions as simple as possible and offer an open line of communication should they require further assistance or information.

Driving a new narrative

The role of the CISO has transformed from an enforcer of rules to an enabler of change. And as organizations increasingly adopt digital solutions, it’s a role that’s more important than ever.

Despite this evolution, many attitudes toward cybersecurity remain unchanged. From the boardroom to the end-user, some still struggle to see the correlation between a more secure organization and a more agile, dynamic, and ultimately successful one.

For cybersecurity to become a vital part of business strategy and company culture, it is up to the CISO to make this connection crystal clear.
Protect is Proofpoint’s annual customer conference and will be virtual this year.

**Why Attend?**
- Hear compelling keynotes from Proofpoint execs and industry experts.
- Participate in a wide range of interactive breakout sessions to take a deeper dive into the topics that interest you most.
- Discover how top cybersecurity and compliance professionals are protecting their organisations with people centric security.

The event is free to attend.

Register here!
[www.proofpoint.com/uk/events/protect](http://www.proofpoint.com/uk/events/protect)

We look forward to seeing you there!
Modern CISO’s Guide to Information Protection

Last year, the pandemic accelerated digital transformation much faster than most organisations were prepared for. Along with remote work came a rapid shift to cloud-based collaboration tools. These two trends created a perfect storm for a rise in insider threats – whether accidental or intentional in nature.

BY MAGGIE FONSECA
Director, Global Programs, Insider Threat Management
Proofpoint
According to a recent study from The Ponemon Institute, the number of insider incidents have increased by a whopping 47 percent since 2018. These incidents cost organizations an average of $11.45 million a year. Here’s why these incidents are on the rise:

- **Hybrid work:** As organizations transition to hybrid work (partially in-person and partially remote), data is no longer protected by the traditional “security perimeter.”

- **New tools:** Insiders are collaborating using a record number of tools, making it increasingly easy to move data.

- **Changing worker profiles:** The profile of an insider includes users outside the company’s typical security controls. Think freelancers, third-party vendors and partners and more.

- **Job-related stress:** Stress can be a major driver of insider threats. Today’s workforce faces job insecurity, caregiving interruptions during the workday, monotonous schedules, and more.

As organisations move into 2021, one thing continues to hold true: only a people-centric defence paradigm can protect both critical information and employees’ privacy.
Here’s a closer look at how Proofpoint Insider Threat Management addresses the three main insider threat types

An insider could be anyone who is close to the organisation. That means an employee, contractor, or even a third-party vendor. Insider threats misuse their authorised access to critical information or systems. Here’s how Proofpoint Insider Threat Management (ITM) can help with the three main types of insider threats.

Accidental insiders: News headlines often focus on sensational stories, such as undercover corporate spies. In reality, 62 percent of insiders accidentally cause incidents. We help by:

- Correlating user activity, data interaction, and user risk in unified explorations and visualised as timeline based views.
- Detecting data exfiltration via risky user behaviour with an easy to use insider threat rules engine and common risk explorations.
- Ensuring your users know what to do when faced with a potentially risky scenario by providing them with targeted security awareness training.

Compromised users: Nearly a quarter of users are compromised, which means they are victims of credential theft via phishing, vishing and other forms of social engineering. We help by:

- Providing the leading threat intelligence built into your DLP to help you understand if data is at risk due to a user whose account has been compromised or is about to be compromised.

Malicious insiders: Only 14 percent of insiders intentionally cause incidents. Malicious insiders are often motivated by financial gain that comes with stealing sensitive data or intellectual property. We help:

- Provide context so you gain instant knowledge of the “who, what, when, why and where” around alerts and what actually happened. You know where files or data originated, where they are moved to, and through what means – providing you with insight into what your end user is doing.
- By correlating your user activity and data movement, your security team is empowered to move quickly to protect against data loss and address insider threats.

Integrating people, processes and technology

Any effective insider threat management program combines people, processes and technology in the right balance. Proofpoint ITM brings together these three elements in one dedicated solution to mitigate people-centric insider risks.

People

Insider threat management programs are made up of people across the entire organisation. Your first instinct may be to isolate this group to security and IT teams only. However, HR, legal, line of business leaders, and executives are equally important players.

Our incident response and case management workflows are tailored for user driven events that require collaboration with teams outside IT and collection of evidence from across the digital productivity stack. Proofpoint ITM can speed time-to-investigate, providing easy-to-consume, visual evidence reports to key stakeholders throughout the organisation.

Key features include:

- Integrations into SIEM & SOAR products
- RESTful APIs to integrate with other systems
- Incident & case management workflows
- Screen capture evidence
Protect against data loss without sacrificing privacy

Maintaining privacy is as much a cultural shift as regulatory compliance. Existing business and technology practices must be balanced with workforce best practices and organizational needs to protect itself. We respect both the interests of employers and the expectations of employees around their personal data and their legal right to access it.

Proofpoint ITM helps you comply with today’s strict data protection and privacy regulations. Here’s how:

- Provides user visibility across enterprise platforms without privacy impact.
- Enterprise privacy capabilities include user anonymisation, Watch the Watcher mechanisms, strong data security, customisable data exclusion policies, role based access controls (RBACs) and a comprehensive audit trail.
- These features enable security teams to meet the organization’s cultural standards and privacy requirements in GDPR, NIST and other cybersecurity regulations.

Process
Implementing an insider threat management program starts with a solid cybersecurity policy, and the ability to enforce it across the organisation.

Proofpoint ITM provides comprehensive detection of risky insider behaviour across unauthorised activity and access, risky accidental actions, system misuse and out of policy data movement. Mature security programs integrate our insider threat intelligence into broader threat hunting programs.

Key features include:
- Policy-based Rules
- Insider Threat Scenario Library
- Threat Hunting
- Anomaly Detection
- SIEM integrations

To learn more, visit:

Technology
Many legacy security technologies focus on data movement alone. To gain visibility into insider threats, it’s important to look at both user activity and data movement together. It’s all about how users are interacting with sensitive corporate data and assets. Monitoring a technology or network perimeter is no longer effective with the rise in remote and hybrid work.

Proofpoint ITM correlates user activity, data interaction, and user risk profiles within a data model that enables analysis and implementation of powerful insider threat detection and response capabilities.

Key features include:
- User Risk Dashboards
- Visibility across endpoint-based activity including application access, data/file interaction, browser usage, endpoint based exfiltration vectors
- Timeline views & visual activity replay
- Reports and analytics
98% of organizations received email threats from suppliers: What you should know

Attackers have turned the supply chain and partner ecosystem into another threat vector. Proofpoint has observed attackers leveraging compromised supplier accounts and supplier impersonation to send malware, steal credentials and perpetrate invoicing fraud.

Proofpoint’s recent research indicates that 98% of nearly 3,000 monitored organizations across the U.S., UK, and Australia, received a threat from a supplier domain over a 7-day window in February 2021. And this is consistent across company size, industry, and country, suggesting that companies of all sizes and industries are exposed to supplier risk and that it’s a universal concern.
What supplier threats look like

Most people think about supplier threats as invoicing fraud. However, our research indicates that attackers use suppliers and business partners to send all types of threats, including phishing for credentials (Account Takeover), malware, and impostor threats like business email compromise (BEC).

The research shows that threats from impersonated and compromised suppliers are more likely to lean on social engineering to prey on human nature, with 74% of threats being phishing or impostor. Less than 30% of threats sent from supplier domains were malware related. The result is further evidence that attackers are targeting people rather than the vulnerabilities of the infrastructure of an organization. In addition, attackers are following suppliers to the cloud and are exploiting popular collaboration platforms such as Microsoft 365, Google G-Suite, and Dropbox to host or send threats at an alarming rate.

Not surprisingly, impostor threats, such as domain spoofing, display name spoofing, and lookalike domains, only account for 3% of total threats sent from supplier domains. Unlike those widespread commodity threats, this type of threat is highly targeted at very few people within an organization.

While email fraud threats are low volume, highly targeted, they often represent large dollar losses. Proofpoint has observed and stopped supplier invoicing fraud attacks in the millions of dollars. In fact, according to the FBI’s 2020 annual Internet Crime Report, Business Email Compromise (BEC) and Email Account Compromise (EAC) scams account for the largest financial loss in 2020, costing the victimized business nearly $1.9 billion.

While no organization is immune to threats from supplier domains, large organizations tend to be targeted more. Not only do F1000 customers receive mail from twice as many supplier domains as the average customer, and thus have greater exposure to threats from impersonated and compromised suppliers, but they are also targeted by a higher proportion of supplier domains. They received over 4 times more messages with threats from supplier domains than the average customer over the 7-day window.
Other findings from our research

The percentages of organizations receiving threats from supplier domains in Financial Services, Manufacturing, Utilities/Communications/Transportation, Wholesale Trade, Construction were 98%, 99%, 98%, 99%, and 100% respectively. The trend is consistent not only across various industries, but also across different regions – 98% of US-based, 100% of Australia-based, and 99% of UK-based organizations have received threats from supplier domains.

There’s no silver bullet for supply chain threats. To better defend against threats from impersonated and compromised suppliers, organizations need a holistic, multi-layered solution. Proofpoint provides a comprehensive, integrated threat protection platform that stops threats sent from compromised or impersonated suppliers, trains end-users to spot and report suspicious email, automates incident investigation and response, and provides visibility into which suppliers pose risk.

### Percentages of organisations receiving threats from supplier domains

<table>
<thead>
<tr>
<th>BY REGION</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>100%</strong> - AUSTRALIA</td>
<td></td>
</tr>
<tr>
<td><strong>98%</strong> - UNITED STATES</td>
<td></td>
</tr>
<tr>
<td><strong>99%</strong> - UNITED KINGDOM</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BY INDUSTRY</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>98%</strong> - FINANCIAL SERVICES</td>
<td></td>
</tr>
<tr>
<td><strong>99%</strong> - MANUFACTURING</td>
<td></td>
</tr>
<tr>
<td><strong>98%</strong> - UTILITIES COMMUNICATIONS TRANSPORTATION</td>
<td></td>
</tr>
<tr>
<td><strong>99%</strong> - WHOLESALE TRADE</td>
<td></td>
</tr>
<tr>
<td><strong>100%</strong> - CONSTRUCTION</td>
<td></td>
</tr>
</tbody>
</table>
Compliance in the age of digital collaboration

The nature of work was already going through a structural shift when a pandemic gripped the world in 2020. More people are working remotely.

Far-flung teams work together across geographies and time zones. And your users – eager to fill in the gaps between email and on-site interaction – are finding new ways to collaborate.

While the global health crisis has accelerated those changes, many are likely to persist long after employees make their way back to the office.

Whether they cluster on premises or interact virtually as part of a distributed team, your people rely on a growing number of digital channels.

Some, such as Zoom, Slack and Microsoft Teams are sanctioned and managed internally. Others, such as social media giants like Facebook, Twitter and LinkedIn, face outward and may be even trickier to manage.

Organizations are struggling to keep up. The sheer volume of content and ever-changing regulations are creating new challenges for compliance and record keeping.

This article explains how to adapt to the changing business landscape. It explores the challenges of capturing and managing a growing volume and diversity of business communications. And it lays out a roadmap for solving today’s thorniest compliance challenges.
The growing demands of
digital communication

In October 2020, Microsoft announced that daily active users on Teams had reached 115 million\(^1\). And Slack added 7,000 customers in just seven weeks after the pandemic pushed people into remote work. The digital sprawl of content has grown exponentially since then. Your employees now use more digital channels beyond email. And that opens a whole new set of challenges. Here are just a few of them:

**Social Media Exposure**

Just like your employees, your customers have gone digital. And many businesses are finding that to succeed in the marketplace, they need to meet them where they spend time. More and more companies are allowing employees – from financial advisors to insurance agents and customer service reps – to represent their business on social media channels and engage with customers and prospects.

But in some industries, this activity is regulated. Organizations are struggling to keep up with changing rules and stay compliant. As your company scales, it must ensure it can apply policies that align with industry regulations – including, FINRA, FDA, HIPAA, FCA, FTC, SEC and others – to avoid fines. Even outside of highly regulated industries, an inappropriate social media post, such as a customer service agent exposing PII or responding poorly to customer complaints, can cost your company its reputation and can ruin customer loyalty.

**Verifying the paper trail for compliance and retention**

For organizations that have compliance in place for digital channels, there is always the challenge of ensuring that the processes they put in place are operating as designed.

And they need a paper trail in case they’re audited or investigated. Building that into a compliance program can get tricky. Even if the software and platforms function efficiently, it is important to monitor for gaps and service disruptions as you capture and manage digital content.

---

1 - “Microsoft say Teams communication app has reached 44 million daily users.” March 2020.
Is your data easy to search and supervise?

Search is not limited to IT teams. Supervision and e-discovery teams need to access communications content too. Making your data easy for them to search will reduce requests and support required from IT. Consider whether these teams can easily search and find:

- Messages from a single person
- Messages between specific people
- Messages from a defined time period
- Topic-based messages
- Platform-based messages

Many communication platforms use SMTP addresses to associate content with users. But some don’t, opting instead for a unique identifier specific to their platform. This approach may affect your downstream process. If your content capture solution doesn’t map the content consistently across platforms, it will take too long and be needlessly difficult to search for content associated with specific employees.

Summary of the three key security and compliance challenges:

- Capturing data across all channels
- Social media exposure
- Verifying the paper trail for compliance and retention

Before you begin tackling these three challenges it’s important to do some discovery work. So, as a starting point consider these key areas to explore:

- How do your people communicate? What platforms are employees using to get work done? Consider channels that have been officially adopted such as Zoom and Slack as well as unofficial channels such as OneDrive.

- How well-equipped are you to handle new types of content? Employees aren’t just exchanging text – they are exchanging videos and graphics too.

- How is content packaged and processed? Gaps and inconsistencies in how content is captured could create problems.

Summary

With the ongoing changes in the way businesses communicate, evaluating how you are capturing and managing all your content across different channels is critical. Help your teams search and supervise content and work efficiently. Make sure all your content is properly captured and tracked.

With thousands of customers worldwide, Proofpoint has a long record of delivering innovative solutions as a service and has been recognized as a Leader in the Gartner Magic Quadrant for Enterprise Information Archiving for nine consecutive years.
Brief history of data
Managing chaos in the digital age

According to some estimates, 90% of the world’s total data volume was created in the last two years. Roughly 2.5 quintillion (2,500,000,000,000,000,000) bytes of data are created every day – an estimated 1.7 megabytes per second per person on the planet.
We’re dealing with more data – and more types of data – than ever. How did we get there? Here’s a brief history of data and how we’re using it.
**BRONZE AGE**
1050 BC - 1609 AD

- **30,000 BC** Oldest surviving cave paintings
- **35,000 BC - 2900 BC** Egyptians invent hieroglyphics
- Sumerians invent cuneiform writing
- **3400 BC** Earliest recorded archive in Sumerian Uruk

**IRON AGE**
1050 BC - 1609 AD

- **1050 BC** Phoenicians develop the first alphabet based on sound.
- **600 BC** Library of Assyrian King Ashurbanipal founded
- **280-250 BC** Library of Alexandria built
- **305 AD** Chinese invent wooden printing press
- **1041 AD** Pi Sheng invents movable type (clay)
- **1400 AD** “Popular prints,” low-quality, mass-produced images, emerge in Europe
- **1455** Johannes Gutenberg develops printing press with movable type (metal)
- **1578** England’s Queen Elizabeth
- **1609 AD** First newspapers

**STONE AGE**
200,000 BC - 2900 BC

- **200,000 BC** Birth of human speech
INDUSTRIAL AGE
1814 AD - 1890 AD

1814 Joseph Nicéphore Niépce creates first photograph
1837 First commercial telegraph installed
1876 Alexander Graham Bell patents the telephone
1877 Thomas Edison patents the phonograph
1890 Herman Hollerith designs a punch card system to calculate U.S. Census. His company later became IBM

MASS MEDIA
1895 AD - 1940 AD

1895 Marconi invents the radio
1909 First commercial radio station goes on air
1928 The "IBM Computer Card" doubles the amount of stored data
1936 Alan Turing presents idea of a computing machine
1939 HP is founded in a Palo Alto, CA. garage
1940 The FCC adopts television transmission standards
**INFORMATION AGE**
1944 AD - 2025 AD

- **1944** ENIAC, the world’s first digital computer is built
- **1946** ENIAC creators launch the first commercial digital computer, the UNIVAC
- **1947** Bell Laboratories invents the transistor
- **1952** IBM introduces the Model 726 magnetic tape storage
- **1958** Jack Kilby and Robert Noyce invent the integrated circuit
- **1959** IBM’s RAMAC computer systems ship with world’s first hard disk drive storage
- **1968** Doug Engelbart unveils a computer with a mouse and GUI features
- **1973** Xerox builds the Alto with GUI features
- **1976** Apple founded

**INTERNET AGE**
1969 AD - 1993 AD

- **1969** ARPAnet, the forerunner of the internet, sends first transmission
- **1971** First email sent
- **1972** IBM invents the floppy disk drive
- **1976** 110 KB 5 ¼ inch floppy disk introduced
- **1982** Industry standardizes the 3 ½ inch “hard-shell” floppy disk
- **1984** Apple launches the Macintosh
- **1987** Toshiba commercializes flash memory
- **1989** Tim Berners-Lee invents the internet
- **1991** Microsoft launches Office
- **1993** NCSA releases Mosaic, the first mainstream web browser.
  - Adobe launches Acrobat (PDF)

**SOCIAL MEDIA**
1996 AD - 2000 AD

- **1996** Mirabilis launches ICQ, the first instant messaging app
- **2000** M-Systems launches USB flash drive
THE CLOUD
2008 AD - 2020 AD...
2008 Amazon launches the Elastic Compute Cloud (AWS)
2009 Microsoft launches OneDrive
2010 WhatsApp launches
2011 Salesforce Chatter launches
2013 Slack launches its collaboration platform
2015 Microsoft launches SharePoint Online
2017 Microsoft Teams launches
2018 Adobe launches Document Cloud
2019 Slack launches its collaboration platform
2020 California Consumer Privacy Act enacted
2021 EU enacts GDPR data privacy rules
2022 Zoom shares soar more than 400% amid Covid lockdowns
2024 Japan amends Act Protection of Personal Information

BIG DATA
2001 AD - 2006 AD
2001 Microsoft launches SharePoint
2002 Reid Hoffman launches LinkedIn
2003 Skype launches video-conferencing platform
2006 Facebook launches
2006 Twitter launches
2008 Microsoft launches Office 365
2018 Verizon launches 5G wireless service
2019 Facebook plans to unify messaging platforms
2020 Brazil enacts Lei Geral de Protecção de Dados privacy rules

ZETTABYTES
ONE ZETTABYTE IS APPROXIMATELY EQUAL TO A THOUSAND EXABYTES, A BILLION TERABYTES, OR A TRILLION GIGABYTES.
When I started working with compliance and archiving products in 2005, I mostly worked with the infrastructure team, specifically the storage and messaging teams. There were two primary use cases for archiving in the early days:

1 **Storage savings and consolidation**: By archiving data from primary storage, you could reduce your storage footprint by “stubbing” email or files. This activity also allowed you to replace the original file with a shortcut (or “stub”). The stub file would link to the original file in the archive and once a user accessed the stub, the original file would be presented. This also allowed storage administrators to move lesser-used data to a lower tier of storage. When prices started to fall for storage platforms, email systems moved away from “single instance storage (SIS)”. Many archiving solutions allowed you to achieve SIS once again, greatly reducing storage requirements.

2 **Server consolidation**: Once data moved from primary storage to secondary storage, the mail servers could realize the benefits of running with much smaller data stores, allowing messaging architects and administrators to run fewer servers. Storage requirements also became predictable based on archive policies, allowing infrastructure planners the ability to avoid surprises in data usage and predictably map out future storage spend.

With these advantages, however, came a few disadvantages. Archive environment upgrades were often very labor-intensive and prone to error. A typical upgrade often involved a very methodical upgrade process that included updating database schema (if not database servers themselves), environment “master” servers, index servers, storage drivers and many other components.
For some of the major revision upgrades, migration to new hardware and operating systems was also required, introducing even more headaches. Merging environments during a merger or acquisition introduced an entirely new set of issues that we won’t even get into in this post.

As someone who worked in the implementation space for many years, working with various legacy on-premises archive vendors, I have witnessed first-hand the processes and resources required to make an upgrade go smoothly. In addition to the efforts required for the upgrade, the fear of data corruption was always lurking. As you planned the upgrade process, you had to factor in a restore from physical disk as a “last-ditch effort” to get the environment back up if something went wrong, assuming you had an uncompromised, recent backup of the archived data and metadata from which to recover. This proved to be a very interesting discussion with customers who had hundreds of terabytes of data in their archives and relied solely on data replication.

### The benefits and pitfalls of E-discovery and Supervision Tools

As communication and collaboration platforms migrated from email to other tools, legacy on-premises vendors were slow to adopt. Some introduced archive connectors for file sharing portals and chat, but those were typically released along with major releases of the archive product. A change in work habits quickly outpaced the release schedules of legacy archive vendors.

Compliance and legal teams learned they could take advantage of the data that lived in this archive. E-discovery and supervision tools were created to use the data in the environment to monitor and search data within the archive. While this new search capability was a big step forward, the lengthy search speeds simply did not meet the needs of modern organizations that needed to improve litigation readiness and address corporate and/or regulatory compliance requirements and audits promptly.

These e-discovery and supervision tools were also very cumbersome to use, so the infrastructure team was often tasked with performing e-discovery searches for the legal team, rather than offering any kind of self-service. In addition, the architecture supporting these tools introduced new levels of complexity and administrative overhead, as solutions were sometimes acquired or developed separately from the archive itself.

### Why Legacy Archive Vendors cannot meet the modern organization’s archiving needs

Content capture and collection needs are changing to the point that legacy archive vendors simply cannot keep up. There is an explosion of data sources and new collaboration tools coming to the market every year. In the last 18 months, I have used three different corporate chat and collaboration tools. How do you stay compliant with change happening this quickly? Waiting for a new major software release to keep you in compliance simply won’t cut it.
Social engagement has also changed the way we work and introduced new requirements to stay compliant. Email, chat, and collaboration platforms are typically under your control, whether they are on-premises or in the cloud. How do you guarantee content capture and control over your company’s brand when it comes to infrastructures that are out of your control, such as LinkedIn, Twitter, Facebook, YouTube and others? Modern, cloud-native archive and compliance tools will help you stay compliant in a rapidly changing world, without the headache of server management, upkeep, and a lengthy and risky upgrade process.

### How Proofpoint solves legacy Archiving Solution pain points

<table>
<thead>
<tr>
<th>Legacy On-Premises Archive pain points</th>
<th>How Proofpoint can help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lengthy and risky upgrades: On-premises archive solutions involve lengthy planning and upgrades are fraught with technical issues. A wide array of internal resources is often required for upgrades.</td>
<td>As a hosted solution, you never have to plan or perform another upgrade. All storage, backup, maintenance, recovery and more are handled by Proofpoint staff.</td>
</tr>
<tr>
<td>Collection and search: Legacy solutions rely on third-party connector platforms to collect data beyond email. Once data is collected, e-discovery and compliance search efforts are inconsistent, often resulting in differing results and search speeds in hours, days, and in some instances, weeks.</td>
<td>Proofpoint’s Content Capture framework includes over 25 targets, including Microsoft Exchange (on-premises and online), Teams, OneDrive, Slack, Yammer and many more. All data that is collected can be accessed by a single federated search with an SLA-backed 20-second result guarantee*, regardless of data size, the number of custodians, or search complexity.</td>
</tr>
<tr>
<td>Reliance on Infrastructure team: These solutions are not user-friendly. Often, members of the infrastructure team must perform collection and search for the legal team.</td>
<td>Proofpoint supports legal and compliance team tools that are easy to use and require no support from the infrastructure team. Our unified interface simplifies processes and grants access to advanced capabilities in the same interface when needed.</td>
</tr>
<tr>
<td>Limited use cases: Slow to respond to the technology and regulatory changes, often releasing new features on a slow schedule that often requires a new upgrade process.</td>
<td>Our solution adapts to technology changes and new information management regulations and policies. Proofpoint can add connectors as needed and utilize e-discovery and supervision solutions for new use cases, such as compliance risk (harassment, intellectual property loss, disgruntled employees), internal investigations and risk mitigation.</td>
</tr>
</tbody>
</table>

*As described in Proofpoint’s Archive Search Performance SLA.*
TOP TIPS FOR HYBRID WORK SECURITY:

Don’t make it easy for Cybercriminals

The world has been thrust into a new way of working. All of us are facing a new normal and when the pandemic is over, the general consensus is that we will have changed our standard modus operandi forever (although exactly how this will impact us, no one can say).

Some professionals, like software engineers and writers, have experience of working from home. But for so many workers, it’s an unfamiliar world. There’s the financial advisor who switched from in-person client meetings to Zoom video calls. Or the dermatologist who’s doing telemedicine for the first time. Millions of educators are navigating online, pretty much learning as they go.

All are facing new logistical and productivity challenges and cybercriminals are leveraging remote working due to COVID-19 by launching campaigns that aim to take advantage of the new reality.

Unprecedented threat volumes

Our threat intelligence team is seeing the cumulative volume of coronavirus-related email lures representing the greatest collection of attack types united by a single theme that they have seen in years, if not ever. This includes attacks that don’t outright mention coronavirus in the subject or body of a message, but instead reference it within attachments, links or lures.

The coronavirus-themed messages we’ve observed are truly social engineering at scale and each is carefully crafted to convince potential victims to click a malicious link, complete a fraudulent payment, or download nefarious attachments. These coronavirus email examples are, at their core, focused on tricking the people receiving these messages based on urgency, fear or the promise of a miracle cure.

To date, we have seen over 500,000 messages, 300,000 malicious URLs, 200,000 malicious attachments with coronavirus themes across more than 140 campaigns (and the number continues to increase). The challenge is that attackers persist in sending COVID-19 related threats because their tactics are clearly working.
Top tips for remote work security

Cybersecurity may not seem like a priority where matters of global health are concerned. On the contrary, it’s more important than ever. Just as we all have a part to play in stopping the spread of a virus, so too does everyone in your organisation have a role in keeping it safe.

Here are some top remote work security tips you can share with your employees today:

1. **Think twice about clicking on links**
   - Phishing emails lead to unsafe websites that steal personal data, passwords, and credit card details. Type a known website address directly into your browser instead.

2. **Confirm all transaction requests via phone**
   - Avoid email scams by verbally verifying that all payment and sensitive data requests are real and authorised.

3. **Use strong passwords**
   - Do not reuse the same password twice. Consider using a password manager to make your online experience seamless, whilst staying safe.

4. **Fortify Wi-Fi**
   - Change the default password on your home Wi-Fi router and enable WPA encryption.

5. **Guard your VPN log-in**
   - Cybercriminals pursue corporate VPN log-ins to directly access all email, data, and cloud apps. At work, confirm remote users are restricted to only necessary systems.
Hybrid work security provides protection for yourself and others

Extra vigilance is required in this new hybrid reality, especially regarding the links you are clicking on, the actions you take or the attachments you open. Remote working can often mean that you are not protected by the same safeguards your office has in place.

It’s extremely important that individuals approach their inbox with the same level of caution that they use in their non-digital, real life. In addition to email caution, if you have a VPN – or better, a zero trust network solution – it should always be turned on and connected. We anticipate threat actors will increasingly pursue corporate VPN log-ins as large parts of the population continue to work from home and a compromised VPN can result in direct access to all email, data, and cloud apps. We recommend configuring VPN for secure remote access so remote users are restricted to only necessary systems.

This new population of remote workers is also faced with something they aren’t used to: many are at home with their family – where they feel safe. We always recommend keeping family members away from your remote office computer, not because they are malicious, but because they haven’t been properly trained by your security awareness department and don’t understand the security controls you should take. This creates the perfect storm for cybercriminals to strike. Don’t make their job easy.
ABOUT PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) is a leading cybersecurity company that protects organisations’ 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 organisations of all sizes, including more than half of the Fortune 1000, 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