ITPro Today™

EXECUTIVE SUMMARY

2019 Threatscape: What to Know, What to Do

Michael Krieger, CEO, MRK Technology Marketing
Ryan Terry, Manager, Product Marketing, Proofpoint

DECEMBER 5, 2018

KEY TAKEAWAYS

- Although security technology is evolving, so are cyber threats.
- Cybercriminals conduct attacks in different ways. Email is their top choice.
- Cybercrimes and data breaches result in costly downtime and reputational damage.
- When it comes to preventing cyberthreats, people are the biggest challenge.
- Cyberattacks now target people, not infrastructure.
- Yet, traditional approaches to information security don't focus on people.
- Proofpoint offers people-centric security solutions.

in partnership with

proofpoint.

2019 Threatscape: What to Know, What to Do

OVERVIEW

The cyberthreat landscape is constantly evolving. Cyberattacks are a reality for organizations of all sizes and in all industries. Many attack vectors capitalize on human error and fallibility. Clicking on a malicious web page, opening a compromised email attachment, or responding to a seemingly legitimate email message can be the first step to financial loss or a data breach. Rather than focusing on firewalls and other aspects of the IT infrastructure, companies must shift their IT security focus to people. People-centric security solutions like Proofpoint are the key to preventing email fraud and other cyberattacks.

CONTEXT

Michael Krieger and Ryan Terry discussed the current cybersecurity landscape and the importance of people-centric security solutions.

KEY TAKEAWAYS

Although security technology is evolving, so are cyber threats.

Security operations center (SOC) technology has evolved. Initially, it was people driven and technology enabled. SOC technology helped people identify policy violations and threats, and then prompted them to take appropriate action. Next-generation SOC technology is technology driven and people enhanced. It relies on automation and incorporates tools like machine learning to flag unusual behaviors. People are still critical to the process, however. They have insight into the business context and possess cyber defense expertise. This new approach to SOC prevents "console blindness," because people are empowered to make key decisions and provide a check on the technology.

Better SOC technology is essential, since cybercrime is constantly evolving. Three trends are:

- **Most cybercrime is financially motivated.** Experts have identified three strategies for deterring these attacks: imposition of financial sanctions, public and private partnerships to disrupt cybercrime tools, and disruption of payment networks run by criminals on the dark web.
- **A cyber cold war is underway worldwide.** As many as 32 nation-states are believed to have the capability to launch a cyberattack. Russia, China, Iran, and North Korea are considered to be the worst offenders.
- **The Internet of Things is raising the threat of cyberattacks.** The potential for cyberattacks is growing as more devices are connected to the Internet.

Given these realities, information security teams are constantly on a state of alert.

Cybercriminals conduct attacks in different ways. Email is their top choice.

Organizations face a wide variety of cyberthreats. Email, however, is the primary vector for launching malware and phishing attacks. Most companies (90%) have seen the volume of phishing attacks either increase or stay the same this year.

Email is also a vector for internal threats, such as careless employees, compromised email accounts, or bad-acting insiders. The rise of cloud-based email like Office 365 has helped cybercriminals. That is because once organizations move email to the cloud, many forget about security. Last year, over 60% of organizations were hit by an attack where malware was spread from user to user via email. About half had infected attachments. Malicious URLs were the cause of over a quarter of the attacks.

2019 Threatscape: What to Know, What to Do

> Over half of all organizations are going to suffer email cyberattacks that negatively impact their business either financially or reputationally.
>
> *Michael Krieger*

In addition to email, other common types of cyberattacks include:

- **Web-based.** Common attack modes are SQL injection, cross-site scripting, and brute force.
- **Social.** Social media–supported fraud is up almost five times since the same time last year. Information available through social media aids with phishing schemes. Between Q2 and Q3 of this year, web-based social engineering schemes grew over 200%.
- **RATs.** Remote access trojans, or RATs, are downloaded with requested programs like games or email attachments. They give cyber criminals admin control over target computers. RATs allow invaders to run key loggers to access confidential information, turn on web cams, format drives, or delete files.
- **Ransomware.** There are conflicting reports about whether ransomware attacks are growing or fading. One source suggests that over the last year, ransomware campaigns like WannaCry have increased. But some reports indicate that ransomware makes up only 1% of the volume of malicious messages.

Cybercrimes and data breaches result in costly downtime and reputational damage.

In 2016, cybercrimes surpassed disasters as the leading cause of data center outages. Experts estimate the average cost of a data breach is $3.86 million.

Data breaches also result in reputational damage and the loss of customers. Typically, organizations with senior leaders like chief privacy officers or chief information security officers experience lower levels of customer churn. These executives direct initiatives that improve customer trust and protection of personal information. Companies that offer identity protection to customers after a data breach also experience lower levels of customer loss.

Many industry sectors are low-hanging fruit for cybercriminals. These include:

- **Banking and finance.** Cybercriminals frequently try to extract money from user accounts.
- **Energy.** Risks to the energy infrastructure have the potential to cross from the cyber realm to the physical world. Large nuclear, coal, or oil plants could be a target.
- **Healthcare.** Both biotech and healthcare organizations are at risk.
- **SMBs.** Small and medium-sized businesses are attractive targets since they typically don't have resources to devote to cybersecurity.
- **Government agencies.** Governments at all levels are seeing a magnified risk of cyber intrusion and data breaches. These can result in the compromise of residents' personally identifiable information, as well as their protected health information.
- **Higher education.** Students are often not cognizant that their online behaviors generate security risks.

2019 Threatscape: What to Know, What to Do

When it comes to preventing cyberthreats, people are the biggest challenge.

Cybercriminals capitalize on human error and fallibility. Ways that people contribute to cybersecurity problems are:

- **Suspiciously registered domains.** "Typosquatting" or URL hijacking relies on user errors. When users mis-type a URL, they are directed to a malicious website. Suspiciously registered domains outnumber brand registered domains 20 to 1.
- **Browser and plugin updates.** These are frequent sources of "malvertising" campaigns. When users install the updates, malware is also installed.
- **Social engineering and phishing attacks.** Over half of all social media texts that impersonate customer support accounts target customers of financial services firms. Dropbox phishing is also a growing trend. Unsuspecting users often fall victim to these schemes.

Cyberattacks now target people, not infrastructure.

The threat landscape has fundamentally changed. Attackers are increasingly targeting people rather than the IT infrastructure. Over 99% of threats rely on users to run malicious code and two-thirds of malicious links are credential phishing.

The shift to the cloud has intensified these trends, creating new threat vectors and data exposure. According to Gartner, email is the most important Office 365 service. Hybrid integration is important, but also a large source of technical problems.

Email fraud has become a board-level issue. According to the FBI Internet Crime Report from summer 2018, there were 78,617 email fraud incidents worldwide between October 2013 and May 2018, which accounted for over $12.5 billion in direct losses. Over 80% of company board members cite email fraud as a top concern for their organizations.

Yet, traditional approaches to information security don't focus on people.

A disconnect exists between the IT security industry and attacker behavior. Gartner's 2017 IT Security Industry forecast predicted that only 8% of security vendors would address email security. However, 93% of all breaches are attacks that target people and 96% of those are via email.

The traditional approach to information security is to invest in firewalls that keep cybercriminals out. Cyber attackers, however, are taking a different, simpler path. They are adept at using LinkedIn and Google to gather personal and professional data. It's easy to take publicly available information and launch an email-based attack that bypasses traditional corporate controls and goes straight to people of interest. This approach increases the likelihood that attackers will successfully obtain money or valuable information. "Very attacked people," or VAPs, have three characteristics:

1. They are targeted by cyber threats.
2. They have access to or manage crucial systems and sensitive data.
3. They work in high-risk ways. For example, they may click on malicious content, fail cyber awareness training, or use risky devices or cloud services.

With email fraud, messages are highly targeted to specific people based on job function or authority level. However, they usually don't include a malicious payload. As a result, there is no malicious attachment to detect, analyze, or quarantine.

2019 Threatscape: What to Know, What to Do

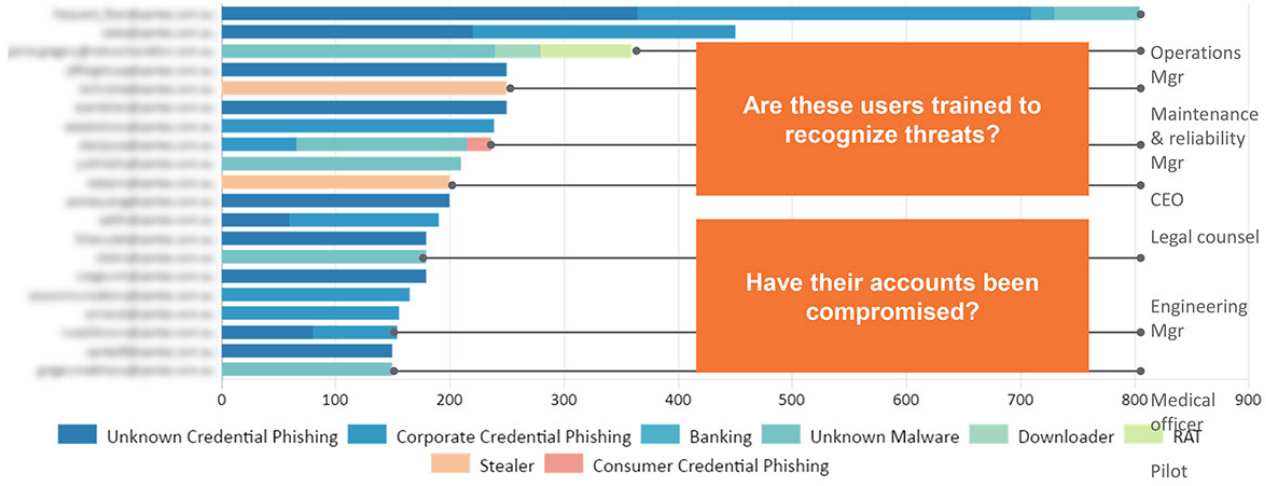
> Attackers use email because it works. If IT security teams aren't focusing on email to the same extent as attackers, they are leaving their organizations open to attacks.
>
> *Ryan Terry*

Proofpoint offers people-centric security solutions.

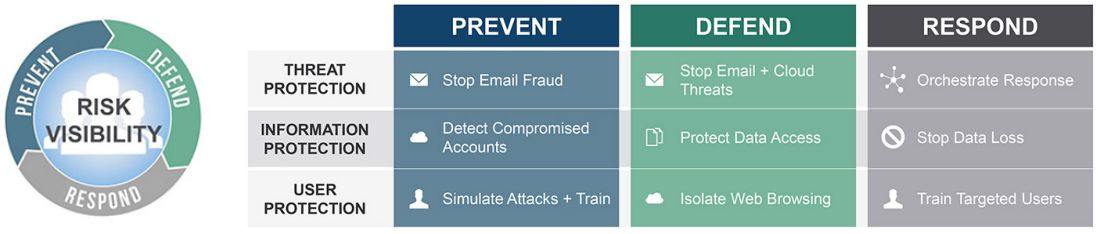
Proofpoint helps organizations gain visibility into their greatest risk—their people—and protects the valuable information those people have access to. Key benefits of Proofpoint's people-centric security solutions are:

- **Identify the targets of cyberthreats.** Proofpoint's VAP View identifies accounts that may be compromised, as well as employees who may need cybersecurity training. In the example below, for instance, the operations manager was the only person to receive a RAT, while the maintenance & reliability manager and the legal counsel were targeted by information stealers.
- **Prevent cyberattacks.** Proofpoint helps organizations stop email fraud, detect compromised accounts, and train employees through simulated attacks.
- **Defend against data and financial losses.** Proofpoint stops email and cloud threats, protects data access, and isolates employee web browsing.
- **Respond to cyberattacks.** Proofpoint enables IT teams to orchestrate an intelligent response, limit the data loss, and train targeted users.

Example of Proofpoint's VAP View



Proofpoint's People-Centric Security



2019 Threatscape: What to Know, What to Do

ADDITIONAL INFORMATION

Proofpoint's quarterly email fraud report. Email fraud impacts organizations of all sizes and in all industries. Each quarter, Proofpoint publishes an email fraud report.

BIOGRAPHIES

Michael Krieger

CEO, MRK Technology Marketing

Michael is a 40+ year technology and marketing veteran with managerial and executive experience in IT, product management, product marketing, market research and analysis. In 2008 he founded MRK, a San Francisco Bay area marketing consultancy that focuses on technology, legal and biotech products. Before launching MRK, Michael spent over a decade as VP of Ziff Davis Market Experts, providing ideation, creation and delivery of integrated marketing offerings for Ziff's largest clients. He has held worldwide marketing roles for Hitachi Data Systems, AST and cloud pioneer FutureLink, one of the first ASPs offering virtual desktop services to a global audience of IT and LOB constituents.

Ryan Terry

Manager, Product Marketing, Proofpoint

Ryan Terry has overseen product marketing for various products within the cybersecurity space for more than 5 years. He currently leads product marketing for Proofpoint Email Fraud Defense and the company's email fraud/business email compromise (BEC) solution.

Ryan received his BS from Arizona State University and holds an MBA in Marketing from Brigham Young University.