proofpoint.

WHITE PAPER

People-Centric Cybersecurity from a Federal Perspective

Bruce A. Brody, *CISSP, CAP, CISM, CFCP, ISSPCS*
Resident CISO, Proofpoint Federal

Introduction

Federal departments and agencies employ millions of personnel to carry out the missions and functions that the American public relies on for its well-being. The federal government provides the operational capability for the world's greatest superpower, providing a wide range of critical missions and functions: providing for the common defense, securing our nation and its infrastructure, conducting our nation's diplomacy, providing care and benefits for veterans, promoting economic prosperity and financial security, creating and maintaining our nation's nuclear capabilities and hundreds more.

All of this operational capability depends on information technology systems and networks. The federal government's information technology systems and networks have been and continue to be attractive targets for foreign intelligence services and other malicious actors in cyber space. Networks that serve hundreds of agencies and millions of employees enable essential government missions and operations, handle sensitive internal communications and store personal information on almost all Americans. Few, if any, parallels in the commercial world exist for the level of threat faced by federal government information technology systems and networks. The confidentiality, integrity and availability of federal information technology is imperative for our way of life and our national well-being.

Table of Contents

The Federal Information Security Modernization Act (FISMA) and Related Mandates

Nearly two decades ago, Congress passed legislation that simultaneously updated the Computer Security Act of 1987 and also formalized the approach to providing system-by-system, site-by-site information security defense for federal systems and networks. The Government Information Security Reform Act of 2001, replaced by the Federal Information Security Management Act (FISMA) of 2002, was a game-changer for federal cybersecurity. The act recognized that information security was vital to the economic and national security interests of the nation. It required each federal department and agency to develop, document and implement an enterprise-wide program to provide risk management and information security protections for the information and information systems that support the essential missions and functions of the department or agency.

Partly in response to increasing numbers of cyber attacks on federal information systems—and also because of the acknowledged flaws of the previous legislation and its implementation—Congress passed the Federal Information Security Modernization Act of 2014, also known as FISMA Reform. As a testament to the acceptance of the importance of cybersecurity by both political parties, the FISMA Reform Act passed the House of Representatives by a vote of 416-0. FISMA 2014 amended FISMA 2002 by reducing the required reporting by agencies and strengthening the continuous monitoring of information systems.

While definitely another move in the right direction for the overall performance federal cybersecurity, the implementation and management of federal cybersecurity improvements, led by OMB and DHS, remains spotty. The Office of Personnel Management breach of 2015, involving the theft of 22 million personnel records by Chinese hackers, and subsequent breaches at the Election Assistance Commission, the Internal Revenue Service, the Federal Deposit Insurance Corporation and the Securities and Exchange Commission continue to underscore the need for a paradigm shift from protecting systems and networks to protecting people from cyber attacks.

Presidential Executive Order 13800 (E.O. 13800) of 2017, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," required agency heads to embrace and be held accountable for risk management of agency systems and networks and mandated that the Cybersecurity Framework of 2014 be used to manage the agency's cybersecurity risk. It also pressed for legacy systems to be retired and for the federal enterprise to be risk-managed as an enterprise, rather than numerous individual siloed agencies.

The Cybersecurity Framework, developed by NIST and known now as the NIST Cybersecurity Framework, is a maturity model broken into five functions of Identify, Protect, Defend, Respond and Recover. Each of these categories has four maturity levels: Partial, Risk Informed, Repeatable and Adaptive. As an enterprise progresses up the maturity ladder from Partial to Adaptive, across all five functions, its ability to manage risk more effectively and improve the overall cybersecurity posture of the organization is appreciable. What's interesting about the Cybersecurity Framework is that, whether intentionally or unintentionally, it is almost impossible for an agency to manage risk across all five functions and at the maturity levels of Repeatable and Adaptive without a heretofore neglected but critically important focus on the creation, development and maintenance of a risk-conscious, security-aware workforce.

People-Centric Security

Federal CISOs have an enormously important job because each is responsible for the risk management and overall cybersecurity posture of the agency's enterprise. The traditional federal cybersecurity focus on systems and networks, while still important, has not appreciably moved the needle on the protection of most federal computing enterprises. While it remains important to update software, retire unsupported legacy systems and patch vulnerabilities, attackers are not using these vulnerabilities the way they used to. In fact, Microsoft reported a 67% decrease in malware infections—specifically on endpoints—in 2019. Meanwhile, software and hardware companies have become better at incorporating core security into their respective development processes, eliminating those easy-to-find vulnerabilities and driving threat actors to research and exploit large, well-funded nation states.

By and large, this is good news and shows the investments in network and endpoint technologies are working to some extent, but it also begs the question as to whether it makes sense to increase investments there in order to decrease the risk of a breach. Does the amount of this investment correlate to the ability to find and mitigate that risk? If history is the teacher, more investment at the endpoint will not appreciably move the risk needle down. According to Proofpoint Threat Research, the massive campaigns of years past are gone and have been replaced by more targeted campaigns.

It is also important to mention the changing world of cybercrime in terms of who is perpetuating these crimes and their motivations for doing so. The cyber-crime landscape, in general, can be broken down into four types of threat actors:

- Cyber criminals
- State-sponsored actors
- Hacktivists
- Insider threats

Cyber criminals range from a few individuals to groups of people with profits as their general motivation. They are either stealing data outright from fraudulent wire transfers or stealing the underlying data and selling it. These malicious actors can be individuals but are most likely criminal organizations.

State-sponsored actors are those nations who use government resources for the purpose of achieving their national security or economic interests. Their motivation is everything from blackmail to using stolen intellectual property for their national gain.

Hacktivists are motivated by social, political or religious ideology. They launch attacks in an attempt to achieve their perverted notion of social justice. They are typically not stealing data for money but exposing that data to cause harm to its owners.

Insider threats come from within an organization. They involve employees that fall into one of these categories: malicious, negligent or accidental. Malicious actors usually pursue monetary gain or revenge.

Proofpoint has been protecting email for 17 years. Our systems handle a significant amount of the world's email every day. We see billions of emails flowing through most the largest internet security providers (ISPs) and domain registrars. With this unique perspective, Proofpoint Threat Researchers, quarter by quarter, consistently confirm that over 99% of cyber attacks are human activated, which means they need a human being to activate the attack by opening a file, clicking a link or being tricked into taking some other type of action.

People have become the weakest link in the cybersecurity chain. The trend also undeniably points to the stark reality that people are attacking people. Unlike past years, the threat landscape is showing fewer high-volume, fully automated attack campaigns, like the Nigerian letter scam or bots and Trojans. In other words, attackers are not just botnets sending massive spray and prey campaigns at scale or using ransomware to automatically encrypt data in order to hold it hostage. Modern threat campaigns are lower volume, highly targeted and *focused on humans*.

Proofpoint has a well-developed and highly capable threat analysis capability—one of the best in the industry—but it is not alone on reaching this conclusion. The most recent Federal Bureau of Investigation (FBI) statistics cite more than $26 billion in losses and more than 166,000 incidents worldwide in 2019 as a result of business email compromise (BEC) and email account compromise (EAC).

Credential phishing is one way that accounts are compromised, but other common ways attackers hijack accounts include password spraying—as in a brute-force attack—or credential-stealing malware. Attackers are not just looking to steal credentials. The real goal is to take over accounts in order to establish persistence and move laterally. This establishes a foothold for cyber criminals and allows them to search for important data and exfiltrate it.

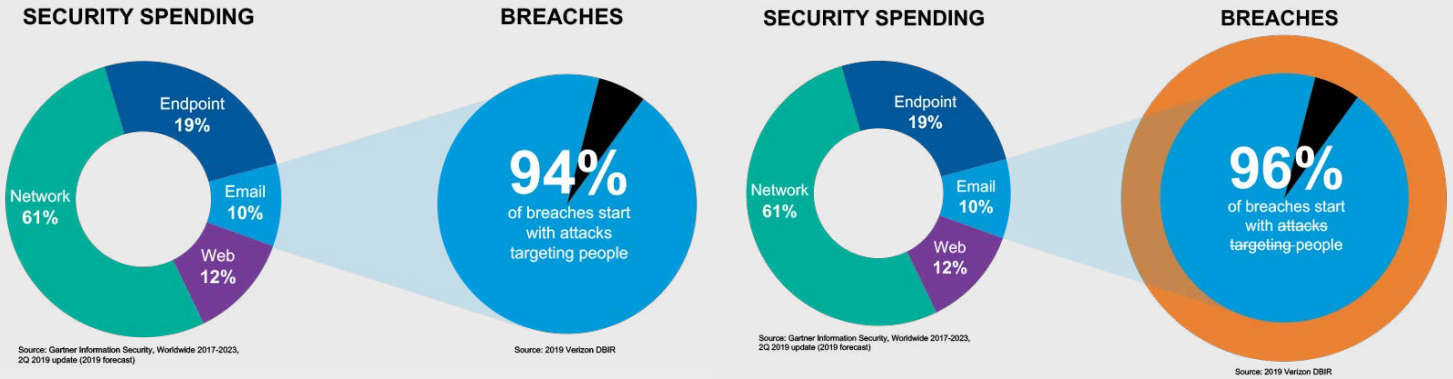
In the past year, Proofpoint threat researchers have also observed:[1]

- 85% of organizations experienced at least one targeted password attack, typically intelligent brute force attacks.
- 45% of organizations experienced at least one successful breach, where an account is confirmed to be acting in malicious ways, such as sending malicious emails or performing mass downloading of files.
- 6% of organizations have a compromised VIP, which means the people who are compromised are typically not executives or those you might think are high-value targets.
- On average, 13 compromised accounts per organization have been breached, so in instances where there are breaches, it's more than one account.

The Gartner data on security spending makes it clear that where organizations dedicate their time, people and money does not map to how they are targeted by attackers.[2] If federal CISOs truly want to mitigate the risk of breach, security attention and resources must shift from focusing on endpoints to focusing on people. Attackers consistently use email as the No. 1 threat vector to launch attacks, primarily because it works. The Verizon Data Breach Investigation Report shows that 94% of breaches start with attacks targeting people via email. If federal agencies are not focused on email and people to the same extent that attackers are, then the probability of a breach is extremely high.

1 Proofpoint Threat Research, Sept 2019

2 Gartner 2019 IT Spending Forecast



Because of this well-documented and thoroughly researched trend of attacks against people, federal CISOs should consider a fundamental shift in how they approach cybersecurity strategy. Most defenders, including most federal agencies, operate with a network-centric point of view with an emphasis on IP addresses, ports and segmentation. Protecting something on the network, such as a server, database or device, is usually handled by putting a firewall in front of it, micro-segmenting it on a VLAN or controlling access to the system via VPN. The adoption of cloud applications and platforms, like Microsoft Office 365, challenges the network-centric approach because it makes it difficult to:

- Gain visibility into all types of threats that affect your people, because threats in the cloud might never traverse the network
- Prioritize alerts and incidents according to relative risk to your organization

Attackers nowadays can easily mine LinkedIn or Google to gather intelligence and launch a targeted threat campaign against any federal enterprise. Moreover, modern attackers do not view the world in terms of a network diagram. At Proofpoint, we help enterprises understand and gain visibility into their greatest risk: people. And not just people, but also the data they have access to and the behaviors that indicate that they might fall for a modern, social-engineered attack. Proofpoint calls these Very Attacked People™ or VAPs.

Most agencies, when tasked with identifying the people they think are being targeted usually mention high-ranking officers like the agency head or C-level agency leadership. In reality, some of those people are being targeted, but the ones that are targeted the most are the VAPs, or the people who have access to the most important data. A VAP could be someone on an important secretive project, someone who has the privileged access to transfer money or someone who monitors the emails and manages the calendars of senior leadership. This people-centric approach to security is essential to managing risk in today's federal computing enterprise. Once an agency understands who is being targeted, the agency can apply mitigating controls to insulate those people.

Proofpoint's proprietary approach to quantifying security risk and understanding the people portion of the attack surface is known as the Proofpoint Attack Index. Proofpoint enables the management of risk by identifying highly targeted people and surfacing the most interesting threats from the noise of everyday threat activity, shrinking the attack surface. The Proofpoint Attack Index can be used to benchmark across users, groups and organizations. It can also tell an agency how attacked the enterprise is in comparison to peer enterprises—for example, if the enterprise is more attacked than other like-sized enterprises or if the CFO organization is more attacked than the CHCO organization. This idea of quantifying and qualifying risk is very important because it means Proofpoint is not just looking at the sheer volume of attacks. Proofpoint truly helps shrink the attack surface.

The days of OMB measuring cybersecurity awareness as one hour of awareness training per person per year are thankfully over. What was once worth a full grade on the annual FISMA report card can now be replaced by the capability to determine who the attackers are targeting, how they are attacking them and providing immediate targeted defenses for the attacked persons. What once was a glaring weakness in the risk management and cybersecurity posture of a federal agency can now become a valuable tool in federal CISOs' defensive arsenal for protecting the enterprise, achieving a higher level of maturity for the Cybersecurity Framework and protecting federal departments and agencies from harmful and dangerous cyber attacks.

About Proofpoint

Proofpoint is a publicly traded (PFPT) pure-play cybersecurity company based in Sunnyvale, California. Our people-centric approach is unique in the cybersecurity industry, and Proofpoint leads the market because of that focus. We protect many of the world's largest, industry-leading customers. And our customers include most of the Fortune 100, Fortune 1000, Global 2000 and thousands more worldwide.

Our deep security DNA is why we're a top cybersecurity company. We've sustained many years of leadership according to industry analysts—no one is close to that. We've appeared in four Gartner Magic Quadrants (MQ): Secure Email Gateway (now a Market Guide), Enterprise Information Archiving, Cloud Access Security Broker (CASB) and Security Awareness Computer-Based Training. Proofpoint has been in the upper right "Leaders" quadrant for several consecutive years.

In January 2020, Proofpoint received FedRAMP authorization for its core email security and archiving products. Proofpoint is committed to providing its state-of-the-practice capabilities to federal enterprise in order to assist in defending our nation's critical computing resources from those who wish to do them harm.

About the Author

Bruce A. Brody is the Resident CISO for Proofpoint's Federal practice. He was the first executive-level Chief Information Security Officer (CISO) in the U.S. Federal Government, and he has also been a CISO in four organizations. He has served as the Chief Information Security Officer (CISO) at the U.S. Department of Veterans Affairs, the U.S. Department of Energy, DRS Technologies and Cubic Global Defense Corporation. He was also a member of the Federal Senior Executive Service, a distinguished manager in the national security community and a decorated officer in the U.S. Air Force.

LEARN MORE

For more information, visit **proofpoint.com**.