



---

# 2016 SECURITY PREDICTIONS

---

AN ANNUAL REPORT  
BY FORCEPOINT™  
SECURITY LABS™



# Table of Contents

## INTRODUCTION

---

| PAGE 3

## PREDICTIONS

01 U.S.  
ELECTIONS

---

| PAGE 4

05 DATA THEFT  
PREVENTION

---

| PAGE 16

02 PAYMENTS  
SECURITY

---

| PAGE 7

06 AGING INTERNET  
INFRASTRUCTURE

---

| PAGE 18

03 ATTACKER  
TRENDS

---

| PAGE 10

07 INTERNET  
OF THINGS

---

| PAGE 21

04 CYBER  
INSURANCE

---

| PAGE 13

08 PRIVACY

---

| PAGE 23

## SOURCES

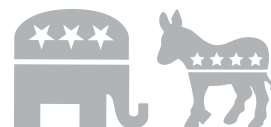
---

| PAGE 25

## Introduction

---

Thought leaders within the IT community are beginning to view cybersecurity not just as part and parcel of the everyday cost of doing business, but as an enabler, a direct driver of business continuity and bottom line growth. This shift in perception has begun to have a dramatic impact on the position and role of security within organizations, from a view of “security means you can’t” to “security means you can.” Over the past year, fences, walls and moats have become outdated as the ROI of security takes priority with a focus on measuring detection, responding to legislation and the automation of remediation, patch management and minimizing dwell time of an attacker. While a lot has changed in 2015, the speed of security means there’s only more to come. These are Forcepoint Security Labs’ predictions for 2016.



## Hackers and Hacktivists Hone In

### BASIS

- Attackers frequently see large events as an opportunity to launch cyberattacks on a curious population.
- Political campaigns, platforms and candidates present a huge opportunity to tailor highly effective lures.
- Candidates' and issues-related websites and social media present a large, built-in following for hacktivists in need of an audience.
- Information on social media is often spread and accepted before fact can catch up with fiction, giving determined hacktivists an opening to misrepresent and/or misdirect the public's perception of individuals and events.
- In political one-upmanship, data often equals an advantage.
- Technology decisions made by candidates during their tenure can expose them to data theft attacks ([as seen by Clinton's use of a private email server](#)).<sup>1</sup>

### PREDICTION

## The U.S. elections cycle will drive significant themed attacks

The Internet, especially social media, are now a standard part of reaching constituents on the campaign trail. Still a relatively new tool in the 2008 U.S. presidential election, by the 2012 election social media was considered a primary communication method (in addition to, if not on par, with traditional news media). This is now a primary vehicle to raise awareness of campaign messages and events, as well as being a way to gauge voter interest and promote engagement on various issues.

The 2016 presidential race will likely see the most prolific use of online and social media campaigning yet as candidates and their teams regularly turn to online resources, campaign websites, Facebook, Twitter and Instagram to reach voters and target specific demographics in their race to win the White House. With 74 percent of adults active on social networking sites as of 2014, [according to the Pew Research Center](#),<sup>2</sup> social media may eventually surpass traditional news media and paid advertising as the top source for voters for election news and opinions.

However, this shift to relying on social sites for news presents challenges. On the one hand, when done right it is a proven method to quickly spread a particular message. The other hand suggests there's little to prevent incendiary, inaccurate information from virally spreading and being accepted by the public as factual. Even if such information is later corrected, this false information lives forever on the Internet, with the potential to inform opinions and as a result misinform – and potentially direct the actions of – the electorate.

---

## *IN POLITICAL ONE- UPMANSHIP, DATA OFTEN EQUALS ADVANTAGE*

---

### **A CAMPAIGN OF LURES AND MALWARE**

Attackers will use the 2016 election and related campaign issues to craft email lures and misdirects in order to push malware payloads with the intent to compromise. Expect lures made to look like political party or candidate email, advocating an online petition or survey about specific election issues, linking to a supposed news story, or relaying information about voter registration or debates.

### **THE EXPLOITATION OF NEW MEDIA**

We've already seen websites hacked to promote propaganda or create confusion. Beginning in 2011, the Syrian Electronic Army (SEA), a group of hackers supporting the government of Syrian President Bashar al-Assad, began targeting and defacing the websites of political opposition groups, government agencies and news organizations with pro-regime commentary. In addition, the Facebook pages of President Obama, along with former French President Nicolas Sarkozy, were targeted by SEA spam campaigns to broadcast support for the al-Assad regime. The SEA also took over the Twitter accounts of legitimate news organizations, tweeting false news updates, creating uncertainty and alarm as the messages spread online before these accounts were again secured.<sup>3</sup>

These attacks demonstrated how relatively simple it was to deface websites and appropriate others' media technology to achieve recognition and reach, even if only temporarily. Other groups may look to follow the SEA's lead in 2016, training their sights on candidates' web pages and social media with a goal to embarrass or discredit, or hijacking the Twitter accounts of legitimate news media to inflame and influence the electorate.

As if to prove the point, only last month the InfoSec Institute released a scorecard indicating which top five presidential candidates is most likely to be hacked.<sup>4</sup> Only one candidate received an A grade, the highest awarded in the study.

### **A FUTURE CYBER WATERGATE**

Nowadays, you don't need to jimmy a lock and rifle through file cabinets for information. Breaking in and stealing or modifying data requires only determination, desire, and a willingness to break the law.

Nation states have been pointing fingers at one another for stealing data from companies and governments for years. Most recently, this activity culminated in the United States and China agreeing in September not to engage in state-sponsored cyber intrusions.<sup>5</sup> However, given the influence the choice of a U.S. President can have, not only on a myriad of social issues and business regulations and operations in the United States, but also on future foreign policy with other nation states, it's not hard to envision a circumstance where factions hoping to gain insight or advantage in an election or following it, might target a candidate or groups involved in promoting them for useful data in keeping ahead of or undermining the competition. However, unlike finding a burglar red-handed, attribution for such an attack will be difficult given the many methods by which hackers can spoof information, circumvent logging and tracking or otherwise remain anonymous.



## TAKEAWAYS

- Businesses should educate employees on the potential for politically targeted and tailored lures in email and via the web.
- Presidential candidates should consider outsourcing ownership of their website donations collections system and web-based advertising to known trusted and respected companies experienced in such activities that use data theft prevention solutions.
- Organizations tasked with hosting a Presidential candidate's website should consider, among other approaches, building the website as secure by design, implement DDOS protection, implement and maintain a Web Application Firewall if appropriate and ensure FTP passwords are kept secure.
- Organizations tasked with administrating the social media accounts of presidential candidates should follow security best practices, including rotating passwords regularly, monitoring status updates, and using suitably complex passwords for log-in.
- Those involved in campaigns or election activity must also elevate the importance of online security in all of their efforts.

## RELATED PREDICTIONS

- Attacker Trends
- Data Theft Prevention



## Pickpocketing the Mobile Wallet

### BASIS

- Money is still the primary attraction for criminal attackers, with credit cards a lucrative historical target.
- Mobile technology and retail innovation is rapidly morphing payments methodology.
- Security is not the first priority for those seeking to alleviate payment friction. Convenience has often trumped security in these rollouts.
- The introduction of the EMV<sup>6</sup> or Chip and PIN standards in the U.S. is likely to decrease face-to-face fraud. However, history suggests that overall fraud rates are not likely to diminish.

### PREDICTION

## Mobile wallets and new payment technologies will introduce additional opportunities for credit card theft and fraud

The payments and payment security landscape is set for some tumultuous shifts to occur in 2016. These seismic shifts are exactly the types of situations from which savvy cybercriminals usually seek to take advantage.

With EMV, or Chip and PIN, technology still in a rolling deployment throughout the U.S., it is still too early to assess its current impact. If historic deployments of this technology are to be repeated, we are likely to see a decrease in the amount of in-person credit card fraud, but overall rates will remain the same as fraud migrates online and into other channels.

As criminals look to shift their game plans, there are three distinct areas we see attackers migrating: newly introduced infrastructure, new payment methodologies and mobile wallets.

### INFRASTRUCTURE ATTACKS

Point-of-sale systems in brick-and-mortar stores are changing in response to rapid EMV implementations. While it may seem that the act of swapping one payment terminal for another is without hazard, the introduction of this new hardware will inevitably lead to security gaps exploited by attackers. This is further complicated by the fact that it can be more difficult to dispute fraudulent charges made using these new “safer” cards.

Integrating new technology and processes securely is a painstaking process. While many will take every measure to do so, the massive scale of change will present significant chances for criminals to attack poorly configured devices, or their network connections. Criminals well versed in physical

tampering of terminals may even take advantage of the migration to “introduce” a number of data capturing devices of their own into a large terminal replacement projects.

#### **HACKING NEW PAYMENT METHODOLOGIES**

While this shift is occurring, there is an increasing push for retailers to take advantage of new technologies to streamline the payment process. The increase in non-traditional payment methods via beacons (a system to allow retailers to detect a mobile app user’s presence in the store) and smart shopping carts will open up the doors for a new wave of attacks. The smart carts and beacons will be a target. Less-rigorous security implementations of these systems will leave them vulnerable.

---

*SMART CARTS AND  
BEACONS WILL BE  
A TARGET. LESS  
RIGOROUS SECURITY  
IMPLEMENTATIONS  
OF THESE SYSTEMS  
WILL LEAVE THEM  
VULNERABLE.*

---

Some banks are already taking action to diminish their responsibility for attacks associated with third-party payment applications that link to accounts at the financial institution. [The Wall Street Journal recently reported](#)<sup>7</sup> that Bank of America has cut off data to some sites and mobile apps that rely on it to provide consumers with money management strategies. While many have chosen to focus on this as a competitive decision, don’t forget the security and liability issues at play. A financial institution traditionally does not hold a consumer liable for fraud committed on their account (business account rules differ). However, if an attacker targeted a third-party application developer, who was in possession of your banking credentials and passwords because you provided them, you may be in trouble with the bank.

#### **PICKPOCKETING THE MOBILE WALLET**

As adoption and the types of transactions capable on mobile phones increases, malware authors will also increase their efforts to steal from a digital wallet. Mobile malware will evolve to use these payment methods to commit fraud. As the cell phone continues to become the preferred two-factor source of authentication for many financial transactions, it has also increased the value of exploiting the mobile device or its applications to empower much more theft than currently seen. Ransomware on mobile may also come as a result of the increased significance of the mobile device in commerce.

#### **HOPPING FROM YOUR HIP TO THE CORPORATE NETWORK**

Once attackers have learned to infiltrate the wallet on your mobile device, they aren’t going to stop there. Remember, money is the primary motivation for these attackers. After they have drained the wallet, they will begin to take advantage of their residency on the device to look for other sources of “income” in the wake of the BYOD phenomena that is now part of the business paradigm. This will likely mean using the device as a head start to compromise your business network; there is plenty more money to be had there for a wizened cybercriminal. Emails, contacts, authentication measures and apps that access the corporate network from the phone can become a phenomenal source of intellectual property, insider information and other confidential business materials become easily obtainable and can net an attacker sizable treasure.





## TAKEAWAYS

- Everyone – not just retailers – must begin to prepare now for protection at the ragged network edge as new mobile and payment technologies stretch and extend the traditional notion of a network.
- The enterprise must acknowledge that the technological push by attackers against the mobile platform to commit fraud will also enable others who wish to breach the enterprise.
- Understanding that the mobile device can create risk and exposure for a business, organizations must look to prioritize the protection of data by monitoring industry best practice and implementing security protections prioritizing data protection.
- Businesses must be forward looking and nimble to accommodate: accelerated update cycles; immediate recognition and categorization of confidential information; rapid security assessment of new technology implementations; and a morphing risk environment.

## RELATED PREDICTION

- Attacker Trends



## .Cyber and .Criminal are Coming for Your .Money and .Computer

### BASIS

- The Internet community has seen a major change in the domain name registration system, with the increased adoption of new generic top level domains (gTLD).
- Attackers are often early adopters of new opportunities and will rapidly colonize new avenues of attack, including new domains.
- As a result, criminals who populate the new top level domains win a much larger proportional presence than in existing, more common TLD.
- This is a demonstrated behavior with all new technologies; when introduced, it is often the fringe elements of the Internet that first move into them.

### PREDICTION

## The addition of the gTLD system will provide new opportunities for attackers

For those accustomed to the old Internet of .com, .edu, .gov, .net, .org, and .info, your intimate little neighborhood is about to get a lot more neighbors. The implementation of expanded new generic top-level domains (gTLD) by the Internet Corporation for Assigned Names and Numbers (ICANN) means that you are now beginning to see many more URLs ending in .club, .xyz and .guru. This will only increase in frequency because as of November 2015, the number of new gTLDs (delegated strings) available is 800.<sup>8</sup> ICANN has reported that 1,300 new names or “strings” could become available in the next few years. A quick look at the new approved and delegated TLD provided by ICANN<sup>9</sup> reveals both big brands big brands used by everyday consumers and common words (including .car, .wine, .mom, .family).

These new TLDs potentially allow for more effective branding and could conceivably become an asset navigating the Internet in the future. For now, they are primarily an asset being cultivated by criminals to confuse users and to ensnare and entrap their computers with malware.

### NEW gTLD = .NEW .OPPORTUNITY .FOR .SOCIAL .ENGINEERING

While there has been a tremendous effort by ICANN to ensure that brands have an opportunity to control the TLD of their names, this hasn't prevented controversy and contesting for specific terms.

---

*DEFENDERS MUST  
CONSIDER HOW NEW  
RESOURCES AND  
FACILITIES MIGHT  
BE ABUSED BY AN  
ATTACKER*

---

Will consumers shopping for a computer steer towards shop.apple, apple.macintosh or apple.computer? Will businesses users with Salesforce accounts respond to an email that comes from renewal.salesforce, salesforce.software or salesforce.updates? This potential confusion is a golden opportunity for criminals and nation-state attackers to create highly effective social engineering lures to steer unsuspecting users toward malware and data loss.

New gTLDs will definitively be used in active spam and other malicious campaigns. In a Forcepoint sample set of several gTLDs, millions of different URLs proved to be suspicious or directly malicious. With attackers well entrenched within the new domains before legitimate users, consumers will eventually hesitate before casual navigation.

These gTLDs will also make it significantly harder for defenders to protect as many are unprepared for the new landscape created. This will prompt security advocates to demand to be involved earlier in the process with how to approach new technologies on the Internet. More specifically, defenders must consider how new resources and facilities might be abused by an attacker.

#### **TAKEAWAY**

- Defenders should recognize that all new technologies hold possibilities for adoption by attackers. Thus, the savvy defender should carefully consider each major change to our ecosystem before waiting for the wave of attacks. This is true at the Internet scale (such as the gTLD example) but also at the company scale (for example, the release of a new feature in a product).

#### **RELATED PREDICTION**

- Payments Security



*The cyber insurance market will dramatically disrupt businesses in the next 12 months. Insurance companies will refuse to pay out for the increasing breaches that are caused by ineffective security practices, while premiums and payouts will become more aligned with the actual cost of a breach. The requirements for cyber insurance will become as significant as regulatory requirements, impacting on businesses' existing security programs.*



— Carl Leonard, Principal Security Analyst,  
Forcepoint Security Labs





## Cyber Insurance Moves Toward “Must Have” and “Evidence Based”

### BASIS

- Still a nascent market, cybersecurity insurance has had to rapidly evolve in the last few years of massive attacks and terabytes of stolen data.
- The “impossible to predict, difficult to understand” nature of cyberattacks creates a real challenge for an insurance industry accustomed to dealing with actuarial data for more predictable risk factors.
- Further disrupting the standard model, different businesses have different levels of online and cyber risk.
- In order to maintain the profitability of issuing these policies, the insurance market will attempt to gain as much real world threat and protection intelligence possible; and to develop minimum level requirements for issuing cybersecurity insurance policies.
- Cyber Insurance for companies will be based on four factors:
  - Market Cap - Representing not only outstanding shares, but the perceived value of the company.
  - Risk Profile - Onsite assessment to determine how prepared companies are to defend against attacks.
  - Targeting Profile - Gathered from multiple cyber companies to determine how often a company is attacked.
  - Responsiveness - How quick companies can shut off breaches, regain control of their companies and eject attackers.
- Over time, cyber insurance will drive improvements in company security posture to better handle threats.

### PREDICTION

## Cybersecurity insurers will create a more definitive actuarial model of risk – changing how security is defined and implemented

2015 was a tough year for breaches and the trend for 2016 looks to be no better. Against this backdrop is the gradual realization within corporations that the value of their company’s data is a large part of corporate assets, and a huge potential cost during a cyber event. Indeed, for some information-centric companies, a data breach can be the largest single risk for business continuity, especially when considering the potential of downstream liability from loss of personally identifiable

information. Such losses comprise not only that data related to customers but also to employees.

**RISK MODEL IS FAST MOVING; IMPOSSIBLE TO PREDICT; DIFFICULT TO UNDERSTAND**

A [November 2015 Wells Fargo survey](#)<sup>10</sup> of U.S. companies with \$100 million or more in annual revenue found that 85 percent have purchased cyber or data privacy insurance, primarily to protect the business against financial loss. Of those with policies, 44 percent have filed a claim as a result of a breach.

A [recent report](#)<sup>11</sup> from market intelligence and ratings services provider Standard & Poor's notes that as successful and financially damaging attacks grow, the cost of cyber insurance could rise or see restrictions. With cyber risk, "fast moving, impossible to predict, and difficult to understand and model,"<sup>12</sup> and exacerbated by companies heavily dependent on the information security of their third-party vendors, deductibles in the U.S. have already climbed to some \$25 million for a \$100 million policy. This has already lead 42 percent of midsize corporations to cite cost as the biggest challenge to purchasing coverage.<sup>13</sup>

Based upon these observations, we expect to see an increasing sophistication in the way the risks associated with a cyber breach are factored into policy cost, just as a driver's safety record and driving habits are factored into the cost of an automotive policy. Insurance companies may even turn to intelligence and security companies to help provide actual data on attacks to develop more consistent, specific actuarial tables and different rating for companies.

**YOUR INDUSTRY AND COMPANY CULTURE MAY INFLUENCE HOW MUCH YOU PAY FOR CYBER INSURANCE**

Not all companies are created equally and not all companies pose equal risk for an insurer. For example, our data clearly shows that different sectors face different encounter rates for threats. [Forcepoint Security Labs' 2015 Healthcare sector Drill-Down](#)<sup>14</sup> showed the industry is much more likely than others to encounter specific threats, including dropper files, lures, redirects and advanced malware.

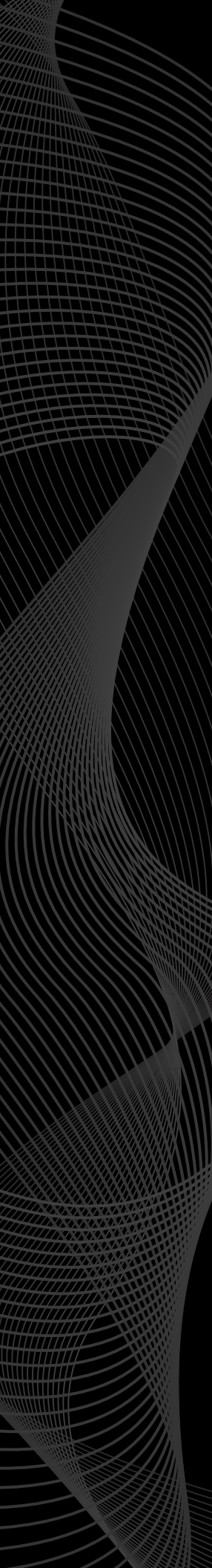
Such sector variation is important, but even within sectors our advanced telemetry shows differences in encounter rates between otherwise identical companies – sometimes driven by attackers, but also sometimes by user behavior. For example, a company may have a culture that tends to visit more "risky" websites, thereby increasing users' exposure. Further illustrating the nonconformity of individual company's security policies, in the Wells Fargo study, one in 10 companies surveyed said they do not have an existing data breach response plan in place while nearly 30 percent did not have employee cybersecurity and data privacy training in place.

We believe that cyber insurance policies will begin to take these variations into account, offering more customized policy rates for those defenders who can demonstrate a better cyber history. Also, based on the actuarial models revised from real world incidents, insurance companies may develop a set of

---

*NOT ALL COMPANIES  
ARE CREATED  
EQUALLY AND NOT  
ALL COMPANIES POSE  
EQUAL RISK FOR AN  
INSURER*

---



security requirements that would be necessary for any company seeking a policy. Requirements for cyber insurance may become as significant a factor as many current regulatory requirements (PCI, HIPAA, ISO 27001). Taking the notion a bit further, we may even begin to see insurers compel cyber audits for compliance to their requirements for a business to gain full policy value. Insurers may also reserve the right to conduct penetration tests to validate the health and effectiveness of the insured, or offer a discount if a third-party penetration test is performed.

Currently, U.S. corporations have dominated the purchase of cyber insurance products,<sup>15</sup> driven by stringent regulations, like the Health Insurance Portability and Accountability Act (HIPAA), aimed at protecting personally identifiable information (PII). But with negotiations in the EU around the implementation of new data protection regulations drawing to a close, adoption of cyber insurance outside of the U.S. will see likely increases, while generous insurance limits currently offered in London markets<sup>16</sup> may decrease as more policies are underwritten.

### TAKEAWAY

- As cyber insurance becomes still more mainstream, savvy defenders should factor in policy costs with defensive posture buying decisions; considering the impact of verifiable security risk exposure, including the third-party continuous monitoring of corporate networks for risky user behavior. Regularly training employees to be smart with email attachments and browsing behavior will be increasingly tied to the bottom line as such programs will be reflected in lower insurance premiums due to reducing their risk of breach. Ultimately, cyber insurance will drive better companies to adopt security postures to handle threats.

### RELATED PREDICTION

- Data Theft Prevention



## Data Theft Prevention (DTP) Crosses the Chasm

### BASIS

- In 2015, data theft seemed like a weekly occurrence, with huge brand names flashed in the headlines.
- Data theft attacks hit a wider variety of industries than ever before, with incidents involving financial services, government, higher education, healthcare and even the security industry.
- The increasing reliance on cloud infrastructure as an integral part of business operations means that much more of the company's confidential data is off-premises.
- An assumption that "we are already compromised" is beginning to pervade security professionals.
- Security pros will welcome data theft prevention products for their return on investment in mitigating the risk of data theft and reducing the period of compromise.

### PREDICTION

## DTP adoption will dramatically increase in more mainstream companies

Chances are, data about you was leaked or stolen in 2015. The variety of industries targeted by attackers in 2015 is unprecedented. Because data has value to criminals, they began to spread their attacks to steal data much more widely than ever before. From retail pharmacy and broader healthcare and insurance industries, to university systems and financial service companies, and even to attacks against prominent security companies, data is money to attackers, and in 2015, they made a lot of money from stolen data.

Simply put: If your company holds information, you have been and will be an attractive target for attackers.

In 2015, price tags for stolen credit card information and identity kits ranged from \$1.5 per record for bulk data rising to the \$20-40 range for "fullz" (name and billing address; credit card number, expiration date and card security code; and Social Security number and birthdate). A complete set of records to be used for identity theft related to health and insurance records can trade for upwards of \$200 dependent on supply and demand. The pricing data certainly suggests that criminals will continue to look not only for credit card data, but more broad personal information. Credit card data and personally identifiable information will continue to be a major target as we roll into 2016.



As a result of these very public breaches, predicted changes in cyber insurance, increased visibility in the boardroom for all things cyber and continued worries about data loss, there will be a more aggressive adoption of data theft prevention technologies outside of its traditional installation base.

### **YOU HAVE ALREADY BEEN BREACHED**

It is now common among security professionals to suggest that organizations practice security with the assumption that the organization has already been breached. Assuming a breach is one thing, but companies with an eye on the bottom line will begin to no longer strive for “perfect protection,” but to highly prioritize the rapid detection of existing and future theft and to make every effort to minimize their window of compromise by remediating not only the threat, but also the root cause.

---

*SIMPLY PUT: IF YOUR COMPANY HOLDS INFORMATION, YOU HAVE BEEN AND WILL BE AN ATTRACTIVE TARGET FOR ATTACKERS*

---

Threats will initially target specific high-value sectors or industries, but will then spread out to attack a broader range of businesses. For example, the healthcare sector will attract more attacks from hackers looking for PII and other information that can be used for health insurance fraud. This will be one of the most attacked sectors, but other industries will soon see attacks as well. Because every company is a target, every company will look to minimize their risk. Security executives, working under the premise that they are already compromised, will investigate technologies that provide the most return on security investment and minimize the risk of data theft. This will lead to a much broader adoption of data theft prevention tools by a broad swath of industries that have recognized that they, too, are a target.

Against this backdrop, we expect attacker behavior to morph as well. The prevalence of DTP solutions will cause sophisticated insiders to conceal, obfuscate and encrypt stolen data, which would render simple “integrated” DTP ineffective.

### **TAKEAWAYS**

- Assume your company is a target for data stealing attacks.
- Adopt a risk-based approach to defense.
- Telemetry shows that DTP solutions can help dramatically buy down risk.
- Start planning for DTP to become a mainstay of a state-of-the-art cyber defense package.
- Carefully evaluate the effectiveness of any DTP solution chosen.

### **RELATED PREDICTION**

- Cyber Insurance



## The Ghosts of Technologies Past will Come Back to Haunt Us

### BASIS

- As our infrastructure ages, the challenges posed by connected technology that has become obsolete will grow.
- This is nowhere more apparent than in the area of cryptography, where algorithms such as MD5 and SHA-1 have become vulnerable to attack.
- As our web infrastructure ages, these changes must be kept up with or else systems that were robust will become vulnerable as a function of time.

### PREDICTION

## Forgotten ongoing maintenance will become a major problem for defenders as maintenance costs rise, manageability falls and manpower is limited

Just like it takes continual effort to keep the Golden Gate Bridge in its famous hue, maintenance of the broader IT infrastructure is an ongoing task and requires continual vigilance and effort. However, unlike a bridge, IT Infrastructure continues to grow and expand in depth and criticality, requiring increasing resources just to maintain the status quo. In essence, with every passing day, IT managers have to work harder just to stay in the same place...and that's a problem.

Akin to barnacles on a boat requiring increased effort by the engine just to stay in cruise, defenders must spend a growing amount of time on maintenance – time that they dearly need to spend on fending off new attacks.

Unfortunately, when it comes to security, keeping up on maintenance is a continual effort where the consequences of failure are far worse than a missing webpage. Instead, attackers continually search for forgotten or abandoned systems, looking to worm their way into the heart of the enterprise. At some point, the cost of older systems that must be maintained will reach a tipping point and become prohibitive. When this occurs, look to vendors to radically restructure their support plans, and aggressively cut end-of-life software support in order to provide service to more recent releases. Updates of operating systems and software that previously were opt-in will now be automatic with no user action. Many software providers will look to this model as patching holes in previous iterations of the system becomes prohibitively costly to maintain.

Our own research supports this. Examining some of the most popular websites in the world, we observed certificate issues related to older hashing schemes such as SHA-1, as well as problems related to the version of ciphers supported. If this were an exam, some of these sites – which one would hope would be scoring a big A+ for security – weren't perfect. These issues trickle down to users. If some of the "big names" on the Internet are struggling to keep up, how can smaller vendors cope?

Compounding the challenge, maintenance of the rapidly aging infrastructure requires significant manpower to remediate. Unfortunately, due to an increasing shortage of good security professionals, the manpower will simply not be there, causing further challenges for defenders, and also for the software and system providers. This shortage of experienced professionals may also result in a number of security snafus by companies trying to rush out fixes in a manner that may be exploited (for example, shipping USB sticks to customers to patch holes or sending emails to inform victims of a breach with links to click).

---

*WHEN IT COMES TO  
SECURITY, KEEPING UP  
ON MAINTENANCE IS A  
CONTINUAL EFFORT*

---

#### TAKEAWAY

- For the defender, the right strategy is three-fold:
  - First, defenders should carefully plan for ongoing security maintenance costs in every development effort, recognizing that these figures could rise as a function of time as the system ages.
  - Second, defenders should make every effort to migrate to current versions of infrastructure products, lest they be taken by surprise when upgrade costs snowball and support dwindles.
  - Third, the security risks by aging systems should be evaluated on an ongoing basis to make sure no loose ends are missed and that the drag caused by older systems is minimized.

#### RELATED PREDICTIONS

- Cyber Insurance
- Data Theft Prevention



*We'll see the Ghosts of Internet Past come back to haunt businesses through compromises caused by old and broken versions of applications, havoc-invoking vulnerabilities in operating system updates and end-of-life processes, and weaknesses in new applications built on recycled code.* ■ ■

— Richard Ford, Chief Scientist,  
Forcepoint Security Labs





## Convenience Meets Continuing Complexities

### BASIS

- The boundaries between corporate and personal devices have become blurrier, causing increasing friction and security challenges affecting critical infrastructure.
- Industries that utilize a large number of connected devices and networked systems in the course of their everyday business, such as healthcare and manufacturing, are likely to face a wider range of security vulnerabilities and threats.

### PREDICTION

## The Internet Of Things will help (and hurt) us all

The websites, apps and electronic devices that comprise the Internet of Things (IoT) make navigating personal and business tasks more convenient than ever, but their popularity also means a wider attack surface, expanse of data and range of vulnerabilities for threat actors to exploit.

### HEALTHCARE IoT SECURITY AILING

Digital and connected diagnostic and screening systems in the healthcare field are expected to reach more than 40 percent global penetration by 2020. While these connected medical devices are invaluable to medical facilities, staff and patients in advancing overall progress and care, they also contain the potential to adversely affect information systems protecting patient safety and data. We are in a climate where up to 75 percent of hospital network traffic goes unmonitored<sup>17</sup> for fear that false positives and delays from well-intentioned security measures could risk necessary and timely patient care. But with healthcare facing 340 percent more security incidents and attacks than the average industry<sup>18</sup>, and no end in sight for the need and number of connected medical devices, reconciling patient needs with network security will become increasingly important. Especially as cyber insurance is likely to become more difficult to purchase without it.

### BUSINESS BENEFIT VS. RISKY BUSINESS

Mobile technologies and Internet connected devices have been a boon for business productivity. Workers are able to access email and business networks on the go in an instant. But many are also doing so in ways IT security may not be aware of, putting their organizations at risk. Still, employees are more often putting the onus on the workplace to protect their privacy when connected to corporate networks, whether they're using personal or corporate-owned devices to do so. Employee training programs and acceptable use policies are likely outcomes of these conflicting priorities.

---

*INDUSTRIES, SUCH AS HEALTHCARE AND MANUFACTURING, THAT UTILIZE A LARGE NUMBER OF CONNECTED DEVICES AND NETWORKED SYSTEMS IN THE COURSE OF THEIR EVERYDAY BUSINESS ARE LIKELY TO FACE A WIDER RANGE OF SECURITY VULNERABILITIES AND THREATS*

---

Devices are also increasingly being used as authentication measures, without similar security controls. For instance, email accessed by phone versus VPN on a laptop. This will require organizations to closely examine all their data and create a balanced, reason-driven, approach to security that is uniform for all elements of their network.

#### **TAKEAWAYS**

- Organizations should aim to rationalize policies between devices for security consistency.
- Companies should be sure to take into account the number and types of devices (and applications) connecting to their network and adjust security parameters accordingly.
- Organizations that have not already should look to institute employee training programs around cyber security best practices as well acceptable use policies to mitigate risk.

#### **RELATED PREDICTIONS**

- Data Theft Prevention
- Cyber Insurance



## Welcome to the Post-Privacy Society. Everything About you is Already Known.

### BASIS

- Increasing frequency of data breaches, such as the many seen in 2015, are changing the way we think about Personally Identifiable Information (PII).
- We are, in fact, moving to a “post-privacy” society, where it is not uncommon for an attacker to have access to information that we have previously considered (rightly or wrongly) as personal.

### PREDICTION

## Societal views of privacy will evolve, with great impact to defenders

The concept of privacy is fluid and changes as a function of time. In fact, the very definition of privacy can be different based on culture, historical period and societal pressures. This is apparent in places such as social networks, where different generations share information in very different ways.

It is not that one generation has “no concept of privacy” – far from it. The truth is that the Internet generation has a different concept of how the personal sphere is to be treated.

It is important to note that it isn't just Millennials shifting their thoughts on privacy. Because the digitization of activities is becoming the routine of life, Generation X and Baby Boomers are also shifting their mores. Whether they know it or not, their information is quietly being gathered by digital devices and everyday activities.

This can become a challenge for businesses as that flow of personal data uses the business' network to move. With the increasing prevalence of BYOD, applications and gadgets that record personal health information and the future potential for connected wearables on your network, you may even have PII in areas you didn't suspect. This mixing of corporate and personal information can become a real mess for the security and compliance officers tasked to sort it out. The popularity of phone fitness and health applications, iHealth, Fitbits (and other autonomous personal data collection applications and hardware) on corporate networks and corporate-owned devices will lead to a broader discussion on privacy and ownership of data.

Some users may not simply accept the End-User License Agreement (EULA) that comes with life's digitation and may rebel. Some, seeking more privacy, may invoke technologies designed to anonymize or encrypt their activities. Using apps, online tools and SSL encrypted traffic, they too will

make it more difficult to enforce policy and security, simply because the business can't see what's happening, again creating a greater security risk.

We believe that data breaches and loss of PII will drive major shifts in the way in which privacy is perceived. Just as the last decade saw the introduction of "the right to be forgotten," we anticipate that within the next decade we will see similar large shifts in privacy rights, especially in the wake of massive breaches of deeply personal data, such as the Ashley Madison or Office of Personnel Management (OPM) breaches.

These shifts are of far more than purely academic interest. For example, the recent "Safe Harbor" ruling has significant implications for companies who transfer data that may include PII between the U.S. and the EU – and this includes security information of the type that is helpful in tracking cyber threats worldwide. In addition, companies should be prepared for regional legislation requirements to significantly complicate international operations in the area of privacy. A seismic shift is coming; like all geological events it may not be quick, but the forces are titanic and will dramatically reshape the landscape for defenders.

#### TAKEAWAYS

- DTP and post-breach activities will become increasingly important.
- Society's shifting privacy conceptions may help or hinder security monitoring, and areas with PII must be watched with extraordinary care.
- While it is hard to be fully prepared for such an unknown, at a minimum defenders must take careful stock of their data handling practices, adopt a nimble footing in this changing landscape, and also make it clear where security practices actually enhance personal privacy rather than erode it.

#### RELATED PREDICTION

- Data Theft Prevention

---

*THE INTERNET  
GENERATION HAS A  
DIFFERENT CONCEPT  
OF HOW THE PERSONAL  
SPHERE IS TO BE  
TREATED*

---



## Sources

- <sup>1</sup> Allen, J. (2015, March 10). Clinton says used personal email account for convenience. Reuters. <http://www.reuters.com/article/2015/03/11/us-usa-politics-clinton-idUSKBN0M61C220150311#7CL0xbGVbSJm6BiW.97>
- <sup>2</sup> Social Networking Fact Sheet. (2015, January). Pew Research Center. <http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/>
- <sup>3</sup> Buchanan, Matt. "Syria's Other Army: How the Hackers Wage War." 29 Aug. 2013. Web. <http://www.newyorker.com/tech/elements/syrias-other-army-how-the-hackers-wage-war>
- <sup>4</sup> Lampe, J. (2015, October 23). Which Top 5 Presidential Candidate is Most Likely to Be Hacked? InfoSec Institute. [http://www2.infosecinstitute.com/l/12882/2015-10-19/zbwt6/12882/121089/2016\\_Presidential\\_Hacks.pdf](http://www2.infosecinstitute.com/l/12882/2015-10-19/zbwt6/12882/121089/2016_Presidential_Hacks.pdf)
- <sup>5</sup> Paletta, D. (2015, September 25). U.S., China in Pact Over Cyberattacks That Steal Company Records. The Wall Street Journal. <http://www.wsj.com/articles/u-s-china-agree-over-cyberattacks-that-steal-company-records-1443205327>
- <sup>6</sup> Welcome To EMVCo. <https://www.emvco.com/>
- <sup>7</sup> Huang, D., & Rudegeair, P. (2015, November 9). Bank of America Cut Off Finance Sites From Its Data. Wall Street Journal. <http://www.wsj.com/articles/bank-of-america-cut-off-finance-sites-from-its-data-1447115089>
- <sup>8</sup> New gTLD registrations top 9M with nearly 800 gTLDs delegated! #ICANN pic.twitter.com/DBvZzQDmNV (Twitter) By: Atallah, Akram. <https://twitter.com/akramatallah/status/661931246189047808>
- <sup>9</sup> Delegated Strings. Icannc.org. <https://newgtlds.icann.org/en/program-status/delegated-strings>
- <sup>10, 13</sup> Cusick, D. (2015, September) Cyber Security and Data Privacy Survey: How prepared are you?. Wells Fargo Insurance. [https://wfis.wellsfargo.com/insights/research/2015-Cyber-Security-and-Data-Privacy-Survey/Documents/Cyber\\_data\\_privacy\\_survey\\_white\\_paper\\_FNL.pdf](https://wfis.wellsfargo.com/insights/research/2015-Cyber-Security-and-Data-Privacy-Survey/Documents/Cyber_data_privacy_survey_white_paper_FNL.pdf)
- <sup>11, 12, 16</sup> S&P Capital IQ, Global Credit Portal (2015, June 9) Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool. Standard & Poor's Financial Services LLC. [http://www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078&SctArtId=320678&from=CM&nsl\\_code=LIME&sourceObjectId=9194506&sourceRevId=12&fee\\_ind=N&exp\\_date=20250609-19:35:11](http://www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078&SctArtId=320678&from=CM&nsl_code=LIME&sourceObjectId=9194506&sourceRevId=12&fee_ind=N&exp_date=20250609-19:35:11)
- <sup>14, 18</sup> Forcepoint Labs (2015, September 23 ) 2015 Industry Drill-Down Report - Healthcare. Forcepoint. <http://www.forcepoint.com/content/2015-healthcare-industry-drilldown.aspx>
- <sup>15</sup> Gandel, S. (2015, January 23). Lloyd's CEO: Cyber attacks cost companies \$400 billion every year. Fortune. <http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/>
- <sup>17</sup> Middleton, P., Tully, J., Brant, K, Goodness, E., Gupta, A., Hines, J, Koslowski, T., McIntyre, A., Tratz-Ryan, B. (2014, October 20) Forecast: Internet of Things, Endpoints and Associated Services, Worldwide, 2014. Gartner, Inc. <https://www.gartner.com/doc/2880717/forecast-internet-things-endpoints-associated>



# **FORCEPOINT** Security Labs™

For more information, visit: <http://blogs.forcepoint.com/security-labs>