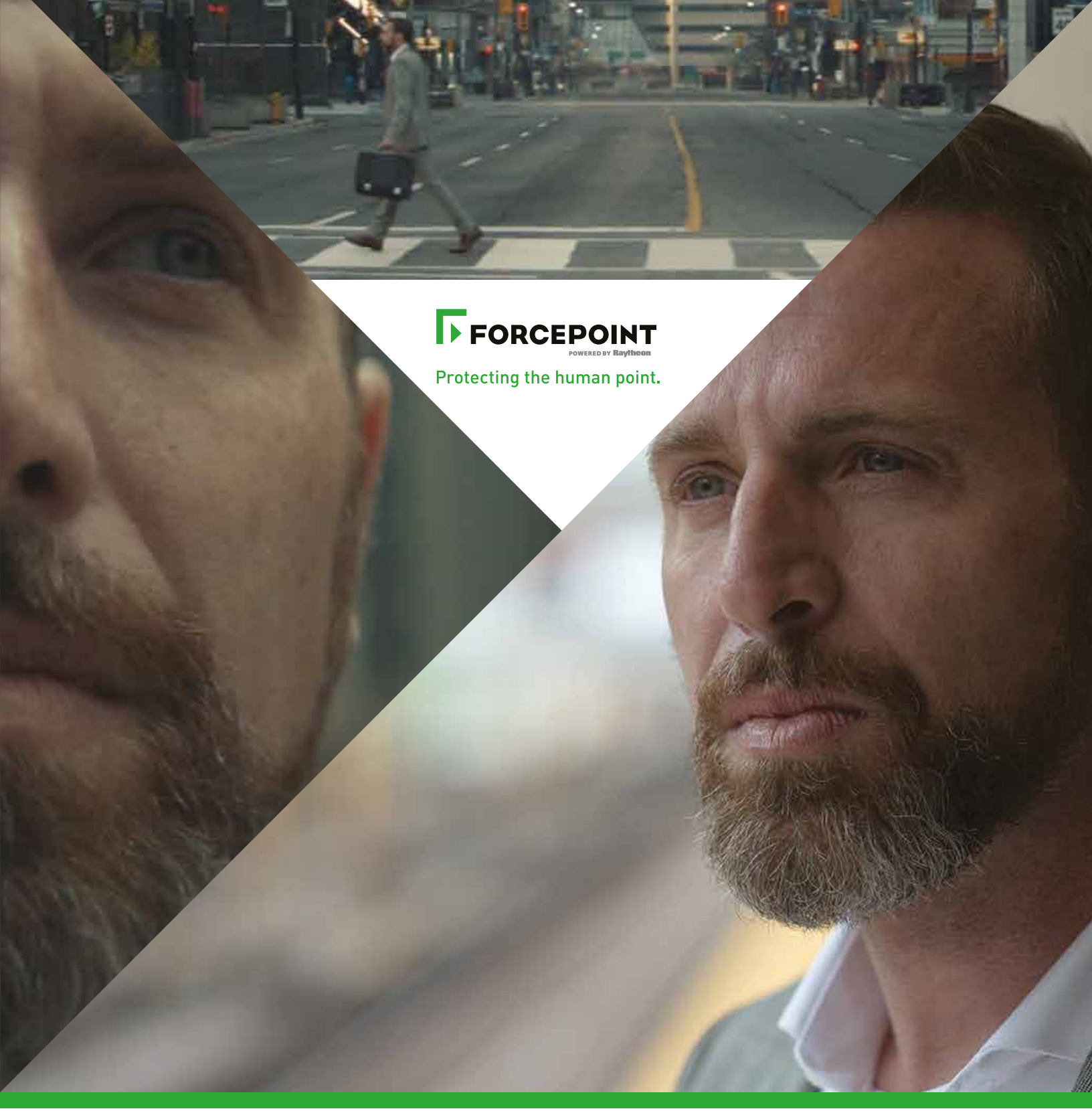


FORCEPOINT
POWERED BY Raytheon

Protecting the human point.

FORCEPOINT Security Labs

2018

SECURITY PREDICTIONS

CONTENTS

INTRODUCTION

A New Paradigm: Human-Centric Cybersecurity

Digital transformation has empowered employees to access and interact with data and intellectual property (IP) through a myriad of systems, applications and devices. However, for too long, the security industry's focus has been on the wrong things. Traditional security perimeters are eroding or becoming obsolete; rather than focus on building bigger walls, the industry needs better visibility. In addition, increases in the sheer volume of data means organizations no longer have the eagle-eyed line of sight over it they once did, leaving them exposed to a slew of vulnerabilities and compliance violations. Understanding how, when and why people interact with critical data, no matter where it is located, is crucial.

We now face behavior-centric risks ranging from the common user error that turns an email lure into a ransomware debacle, to sporadic, anomalous activities that, once presented in context, can illuminate the early stages of a malicious insider threat. In a world where malware is continually evolving, critical data is moving to the cloud and criminals are exploring new vectors of attack, how can security professionals stay up to date with, and keep ahead of, changes in the industry?

To assess cyber risk in real time, we must remain vigilant of data as it moves across, as well as into and out of, the enterprise. By understanding how data flows, who has access to it and why, we can increase the efficacy of security; by homing in on normal and irregular data and user patterns, we can reduce complexities, and focus on the events that really matter.

In this report, we describe major security shifts we expect in 2018. At the heart of many of these predictions is a requirement to understand the intersection of people, critical data and IP – the human point. By placing behavior and intent at the center of security, security professionals can keep up with technological innovations to come.

PRIVACY FIGHTS BACK

Privacy makes a comeback with support from new regulations

In 2015[1], we predicted that users' perceptions of privacy would begin to change, as individuals struggled to understand how to live and thrive in a "post-privacy" society. The last two years have seen a steady erosion of the clean line between the personal and public sphere – even ISPs have the legal right to sell customer data. Furthermore, ongoing geopolitical uncertainty, and threats both foreign and domestic, highlight the perceived tension between individual rights and security for all. To date, privacy has not put up much of a fight; that will change in 2018.

Our prediction is based upon what we see as the perfect storm between four drivers: legal, technological, societal and political. The confluence of these factors will cause a tectonic shift in the privacy landscape.

REGULATIONS PAVING THE WAY

Legal concerns lead the pack in terms of visibility in the security community – most recently under the heading of the General Data Protection Regulation (GDPR), though this is far from the only piece of legislation that impacts how companies handle personal data. With regulations set to come into effect on May 25, 2018, privacy is top of mind for many technologists. Compliance will drive visibility through 2018 and beyond.

"The stars are aligning to make 2018 the kick-off to what we're going to call "The Privacy Wars" – pitting technologists against the ordinary person on the street, and splitting opinion in government, at work, and at home."

DR. RICHARD FORD
CHIEF SCIENTIST

REGULATIONS AND GUIDELINES PROTECTING PEOPLE'S PRIVACY INCLUDE:

The GDPR, a European-led regulation that will affect global businesses that hold or process the personal data of any European Union resident.

EU ePrivacy Regulation, which covers confidentiality of information, treatment of traffic data, spam and cookies and which will be updated to come into line with the GDPR. This will impact cloud service providers and cross-border transfers of data worldwide.

NIST Special Publication 800-171, a requirement on suppliers to U.S. federal organizations to adequately protect controlled unclassified information (CUI) including the privacy of personal data for which they are responsible.

SOCIETAL CHANGE

Technological and societal changes are two other major factors. Individuals are used to trading convenience for privacy as they use location-based and ID-tracking services on mobile phones and home assistants, and predominantly accept this in their private lives. In the workplace, the benefits of a more human-centric approach to security, which focuses on the interaction of people and critical data, will lead to increased data collection ongoing.

Despite the importance of both of these areas, the social shift is the most interesting. Here, large-scale data breaches (like Equifax) raise the level of awareness in the general community and shine a light on the role of data aggregators. And, since breaches like Equifax impact the average person, privacy has moved from an abstract concept to something actionable.

GOVERNMENT INVOLVEMENT

Lastly, the geopolitics of 2017 cannot be ignored. The world seems less stable, and the rise of populism in the West coupled with ongoing terrorist threats highlights the uneasy tension between individual privacy and national security. This has given rise to continued discussions by governments on encryption and its role in a free society.

Each area alone could make 2018 an interesting year from a privacy perspective, but together they will ignite discussions on a political, enterprise and personal level. Unfortunately, our assessment is that these discussions will be more polarizing than unifying, making little progress toward reconciling legitimate privacy concerns with genuine security needs.

PREDICTION

2018 will ignite a broad and polarizing privacy debate not just within governments, but between ordinary people.

GDPR: PROCRASTINATE NOW, PANIC LATER

The EU regulation marks a point of no return for personal data controllers and processors

Linked closely to our privacy prediction, we anticipate changes to data protection in 2018. When the EU General Data Protection Regulation (GDPR) becomes enforceable by law in May of 2018, it will require global organizations that hold the personal data of European Union residents to adhere to new requirements around control, processing and protection.

CLEAR REPERCUSSIONS FOR NON-COMPLIANCE

Along with the new regulation comes additional legal liability; the penalties for non-compliance will be immense. Once the GDPR legislation becomes enforceable, any personal data breach[1] impacting a European Union resident will need to be reported within 72 hours; companies that do not comply will face fines of up to 20 million Euros or 4 percent of global turnover, whichever is higher.[2] Those who have not budgeted for the long-term implications of the GDPR will struggle.

Organizations will be watching closely for the first milestone case to understand how local Supervisory Authorities (SAs) will treat infringements, whether initial penalties will be light, and who will be made an example of.

"It will become apparent to organizations that the stop watch will start in May of 2018. It is not a race to the finish as there is no finish line – the finish line will keep moving due to changing legislation and attack trends."

NEIL THACKER
DEPUTY CISO

THE REGULATION'S FAR-REACHING IMPACTS

The EU is the world's second largest economy and a leader in the digital economy. The GDPR may be the first regulation to set the bar so high, but other countries will follow the EU in terms of updating their regulations to match this new standard for data protection.

The definition of "personal data breach" within the GDPR is also interesting and has repercussions for the industry. As "breach" is defined as "leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed," under the regulation, a ransomware attack that encrypts personal data would still be considered a breach, even though the data is not actually stolen. As such, we expect a GDPR case to apply to a ransomware incident in the immediate months following enforcement of the regulation.

As significant as its fines are, the GDPR has a more important characteristic: it offers data subjects transparency into how their information is processed. The regulation specifically offers rights to obtain confirmation that their data is being processed, access to their personal data and rights to objection, rectification, erasure, portability and others.

PREPARATION FOR THE GDPR IS CRITICAL

Somewhat of a precursor to the GDPR, the Dutch Data Protection Authority (Dutch DPA) received more than 1,000 breach notifications in the first 100 days of the implementation of its data breach notification law. In this same vein, the majority of businesses will be stunned by the regulation's impact on their operations, as it creates security challenges that cannot be solved solely with technology.[3]

This will drive international businesses to closely examine their security incident response and reporting processes. Smart companies will see this not just through the compliance lens but as a feature of their security policy. Some CISOs will pivot towards mitigation rather than detection or protection, and will implement improvements to controls and response to better ready their business for the GDPR deadline.

However, as the GDPR deadline approaches, panic will ensue as the majority of procrastinators realize that GDPR compliance requires more than anticipated, and will overcorrect by applying policies that stifle business processes. We will see many organizations undergo CISO reshuffles as these individuals realize they are unprepared and seek other roles to avoid internal criticism.

PREDICTION

Most organizations will not be ready prior to the GDPR enforcement date, and panic-driven policies will stifle businesses as they struggle to become compliant.

DISRUPTION OF THINGS

IoT becomes a target for mass disruption

The popularity of the Internet of Things (IoT) has become increasingly evident over the past year: Gartner forecasts 8.4 billion connected things will be in use worldwide in 2017, up 31 percent from 2016.[4] A threat that will emerge in 2018 is "the disruption of things," particularly relevant within enterprises where logistical and supply chain sensors and healthcare devices are critical parts of infrastructure.

IOT'S RAPIDLY EXPANDING ATTACK VECTOR

The widescale adoption of IoT devices in consumer and business environments, coupled with these devices often being both easy to access and unmonitored, makes them an attractive target for cybercriminals wishing to hold them to ransom or obtain a long-term, persistent presence on the network.

IoT security must be viewed from three vantage points: securing IoT devices, broader IoT systems (and devices connected to those networks), and the data leveraged or transmitted by IoT devices. Whether an IoT device or a broader IoT system, data is at the core, as devices or systems without data are useless. As the number of IoT devices grows and interconnections multiply so does IoT malware, which nearly doubled from 2015 to 2016.[5,6]

This is particularly relevant within those organizations with critical infrastructure that can access proprietary or personal data.

"We must identify the difference between genuine connected devices accessing critical data and malicious acts, be they the result of cybercriminals using stolen credentials or an automated piece of malware behaving like a user."

LUKE SOMERVILLE
HEAD OF SPECIAL INVESTIGATIONS, FORCEPOINT SECURITY LABS

ENDLESS POSSIBILITIES FOR DISRUPTION

While ransomware of things is feasible, we believe it remains unlikely for 2018. However, the internet of connected things offers access both to massive amounts of critical data and to "the disruption of things." For example, it will be possible for any attacker with disruption in mind to steal credentials or insert malware into systems and:

- Infiltrate a network of connected refrigerated trucks and raise the temperature, spoiling food and disrupting social infrastructure;
- Take down a network of insecure home internet routers;
- Build a larger, more powerful botnet of things to extract data or demand ransom.

CONSUMER DEVICES WILL NOT BE HELD TO RANSOM

While possible, attackers holding a household's internet-enabled devices to ransom is unlikely, since the type of data held on consumer devices isn't exceptionally valuable compared to other targets. Home devices are typically small, relatively low-cost and generally not worth paying the ransom for (if a ransom message could even be displayed). Automobiles present a potential attack surface, but this issue can be remedied with relative ease via over-the-air updates, which are currently being implemented by major car manufacturers.[7]

ADDITIONAL STEPS MUST BE TAKEN TO PREVENT IOT VULNERABILITIES

The IoT industry has not learned from previous security missteps, like the one stemming from the discovery that smart meters installed by utility companies in Spain could be hacked to under-report energy use.[8] In the future, this kind of poor protection against tampering could eventually lead to the systematic shut down of power across a wide area. We will also see integration of a man-in-the-middle (MITM) attacks into IoT networks. As more connected devices, such as home personal assistants, have financial data associated with them, they become more attractive and lucrative targets for attackers.

PREDICTION

IoT is not held to ransom, but instead becomes a target for mass disruption.

THE RISE OF CRYPTOCURRENCY HACKS

Attackers aim to capitalize on digital currency explosion

A reported 1.65 million computers are used to mine Bitcoin, the digital currency with a market capitalization of more than $107 billion USD. Cryptocurrencies have quickly become the payment method of choice for cybercriminals seeking a ransom.[9] While the principle of Bitcoin's underlying blockchain technology makes the insertion of falsified transactions into historical blocks prohibitively difficult, cybercriminals will instead turn their attention to vulnerabilities in its supporting systems, including those used to create digital currency transactions.[10]

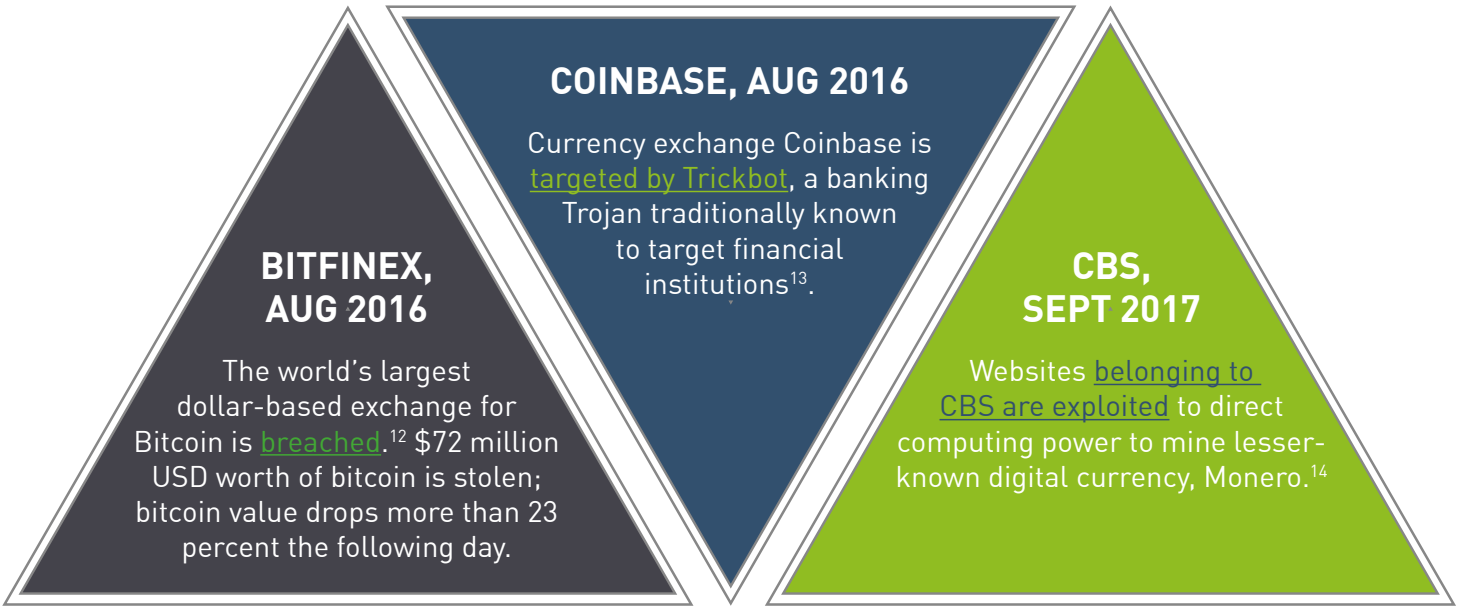
DIGITAL CURRENCY EXCHANGES ARE A HOTBED OF RISK

While cybercriminals are not likely to succeed at attacking its underlying encryption in the short term, malware authors have already configured malware to mine cryptocurrency, steal currency from cryptocurrency exchange users' wallets and exploit weaknesses in blockchain's underlying algorithms.[11]

We expect to see an increasing amount of malware targeting the user credentials of cryptocurrency exchanges and the websites that allow users to buy, sell and exchange crypto-currencies for other digital currency or traditional currency.

"Compromising the systems used to make cryptocurrency transactions will be an attractive proposition for highly skilled attackers."

LUKE SOMERVILLE
HEAD OF SPECIAL INVESTIGATIONS, FORCEPOINT SECURITY LABS



GOVERNMENT REGULATION AWAITS

Blockchain technology underpins the transaction ledgers used by most cryptocurrencies. Governments around the world are seeking to legislate and therefore control the providers and users of blockchain-based technologies.[15] The U.S. Department of Defense (DoD) was recently tasked with investigating the potential impact of blockchain compromises following the passing of a bill by the U.S. Senate; its findings will increase demand for more robust security.[16]

PREDICTION

Attackers will target vulnerabilities in systems that implement blockchain technology associated with digital currencies.

DATA AGGREGATORS

Cybercriminals seek a personal data payday

Cybercriminals target complete sets of information such as personal data from banks and electronic health care records due to their undeniably inherent wealth of value. This data is not something that can be changed or adapted like a password; rather, it is always associated with an individual. It's not surprising that data aggregators in the public and private sector represent the path of least resistance to the greatest reward. Just as we saw with Equifax, a weak link in a system containing an abundance of personal identifiable information will be exploited.[17]

EQUIFAX WAS THE TIP OF THE ICEBERG

The Equifax breach was the first of such magnitude on a hosted business application, but it will not be the last. At risk are those applications that contain information on a sales force, prospects and customers, or those that manage global marketing campaigns. The Equifax breach in September of 2017 was, in fact, the second breach reported by the credit bureau; the first came months earlier, in March of 2017, which it failed to disclose until late August.[18] This sort of disclosure lag time is just one issue the GDPR aims to resolve for European citizens.

Concerned with the implications of sharing login credentials with third-parties, banks and other financial institutions have previously warned they would not be held liable[19] if their customers shared account access with third parties such as Mint, a free web-based financial management service. The targeting of large-scale databases has even been attributed to nation-state cybercriminals. One instance of this occurred when cybercriminals, believed to be working for the Chinese government[20], compromised the Office of Personnel Management, which holds data on countless U.S. federal employees.

"Because aggregators hold huge quantities of data and have so many ingress and egress points, their complexity creates security challenges. These types of breach incidents have caused significant concerns to consumers – and the full impact has not yet played out."

NICOLAS FISCHBACH
GLOBAL CTO

ANYTIME, ANYWHERE ACCESS – AND ANYTIME, ANYWHERE EXPLOITS

Modern working practices rightly allow anytime, anywhere access to data by employees and authorized third parties (including APIs); data aggregators offer efficient and effective ways of working that companies and their customers have wholeheartedly adopted.

The Equifax breach is a wake-up call for businesses worldwide, which must improve security systems to meet attackers taking aim at these data goldmines with increased resistance. Working harder is not possible, but working smarter is. Examining the flow of the data through an organization is the only scalable defense mechanism, and by looking for and spotting uncommon consumption patterns or the misuse of account credentials on a database, malicious behaviors can be identified.

One of the following attack vectors will likely be targeted in 2018: an exploit of known vulnerabilities; accidental compromise via employee error; third party compromise leading to first party breach; a ransomware or social engineering attack; exploits of security misconfiguration; and exploits of weak authentication practices.

PRESSURE WILL BUILD FOR DATA AGGREGATORS

Credit reporting agencies, online retailers and other large aggregators of data will come under mounting pressure to better communicate with the general public. They will have to more fully disclose the types of personal data they have amassed, explain when and how that information is used, shared or sold, and begin to offer certain controls on distribution and use. Unified breach disclosure requirements and product security warranties will follow. No one is too big to fail.

PREDICTION

A data aggregator will be breached in 2018 using a known attack method.

CLOUD SECURITY

Cloud admin is the new domain admin

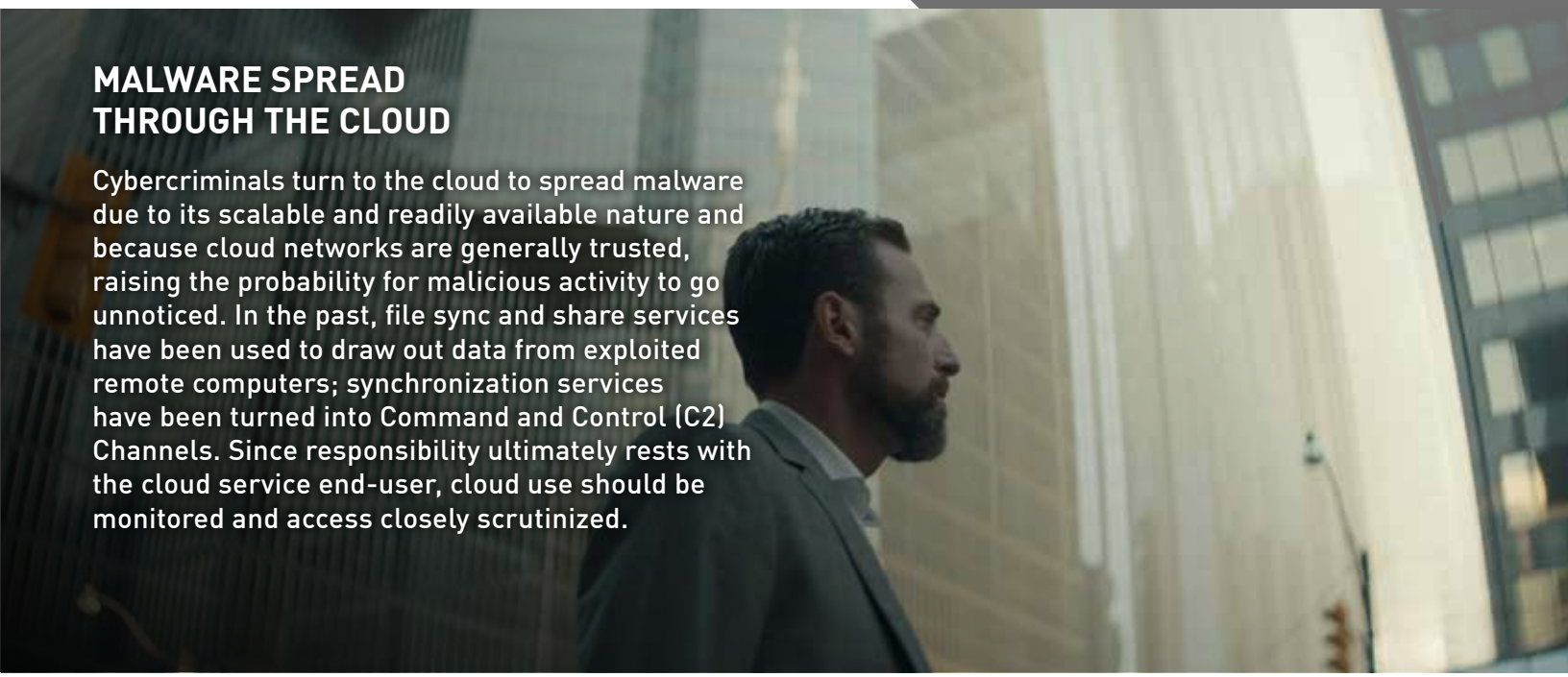
The shift to the cloud has occurred at an astronomical rate, with high reported growth in vendors selling infrastructure-as-a service (IaaS) like Azure and AWS and those deploying software-as-a-service (SaaS) apps, such as Box and Salesforce. This is similarly the case for Microsoft Office 365, which has seen strong upticks in user base and will cross the 100 million user threshold sometime in 2017.[21] Since a compromise of cloud credentials essentially grants access to a wealth of critical data, adoption of cloud technologies **increases the risk of a breach from a trusted supplier** or a trusted insider who is compromised in some way.

EMPLOYERS LOSE VISIBILITY OF DATA IN THE CLOUD

New applications are introduced into organizations every day, unbeknownst to IT. For large enterprises, 30 to 40 percent of IT spending comprises shadow IT, in this case unsanctioned cloud services.[22] And while cloud vendors are generally secure, they are not custodians of customer data and don't have any say in how their customers protect their data.[23] While existing infrastructure can be leveraged in combination with the right cloud security tools to help enterprises discover cloud apps, they don't provide the visibility and control required for a comprehensive solution.

"If an employee accessed a cloud app through public Wi-Fi, and the username and password were intercepted, how long would it take before anyone realized it? Securing data in the cloud requires a strategy for insight and protection that has to account for the risks posed by users."

CARL LEONARD
PRINCIPAL SECURITY ANALYST



MALWARE SPREAD THROUGH THE CLOUD

Cybercriminals turn to the cloud to spread malware due to its scalable and readily available nature and because cloud networks are generally trusted, raising the probability for malicious activity to go unnoticed. In the past, file sync and share services have been used to draw out data from exploited remote computers; synchronization services have been turned into Command and Control (C2) Channels. Since responsibility ultimately rests with the cloud service end-user, cloud use should be monitored and access closely scrutinized.

SUPPORTING CLOUD-FIRST INITIATIVES

When it comes to SaaS — where arguably the service provider has more responsibility around security and embedding it into the application than the end-user — there are still areas where end-users could apply security monitoring and control to protect sensitive data or look for malware.

Organizations will soon support cloud-first initiatives through human-centric security programs, beginning with an understanding of typical user behavior or data usage patterns, which makes it possible to flag risky behavior or abnormal usage of cloud applications. Organizations will conjoin these training programs with Cloud Access Security Broker (CASB) technology to help identify risky users and applications.

PREDICTION

Adoption of cloud technologies will increase the risk of a breach from a trusted insider.

ENCRYPTED BY DEFAULT – IMPLICATIONS FOR ALL

Attackers follow the mass migration to HTTPS

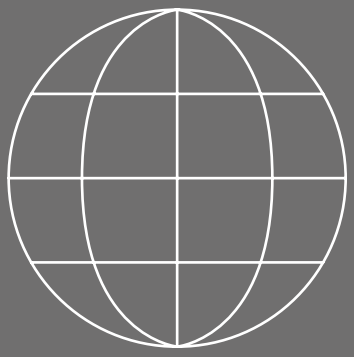
The web is moving to encrypted-by-default.[24] Seventy of the top 100 non-Google websites, accounting for 25 percent of all website traffic, are using this technology. This includes major global search engines, social media networks and e-commerce websites, which are investing in the technology to make the web a safer place for consumers. In reaction to the increased use of HTTPS, cybercriminals and nation state actors are adapting their tactics, techniques and procedures. For example, scammers have been acquiring certificates that make their fraudulent websites imitate the likes of PayPal and Google to appear legitimate.[25]

SECURITY WILL INCLUDE HTTPS INSPECTION/DECRYPTION

In order to protect personal data and intellectual property, organizations are using SSL/TLS decryption and inspection technologies on their web and app traffic, simply to understand the data moving from machine to machine. Such technologies use man-in-the-middle (MITM) techniques in a legitimate manner. The MITM stream is the only effective way to monitor the traffic for network Data Loss Protection (DLP) and Cloud Access Security Broker (CASB) analysis; therefore, this will become more common for legitimate purposes – and will raise privacy challenges. The visibility that MITM provides means malware will be designed to take this into account when determining how to act, by ceasing execution once it realizes it is under analysis.

"While there are legitimate man-in-the-middle (MITM) techniques, we'll see malware attempting to detect or thwart MITM security by using non-standard cryptography, certificate pinning and other techniques."

AUDRA SIMONS
HEAD OF
FORCEPOINT INNOVATION LABS



Seventy of the top 100 non-Google websites, accounting for 25 percent of all website traffic are using HTTPS by default.

THOSE NOT USING HTTPS INSPECTION/ DECRYPTION ARE AT RISK

Malware creators or those controlling botnets will continue to take advantage of any environments not using SSL/TLS decryption and inspection to hide communications using encrypted communication channels. We will also see other malware attempt to detect or thwart MITM security techniques by using non-standard cryptography, certificate pinning and other techniques. For example, the Shifu banking trojan cuts communication with its command and control servers if it observes that MITM interception is occurring on the connection.[26] To avoid these risks, HTTP Strict Transport Security (HSTS) allows web servers to declare that web browsers (or other complying user agents) should only interact with it using secure HTTPS connections.

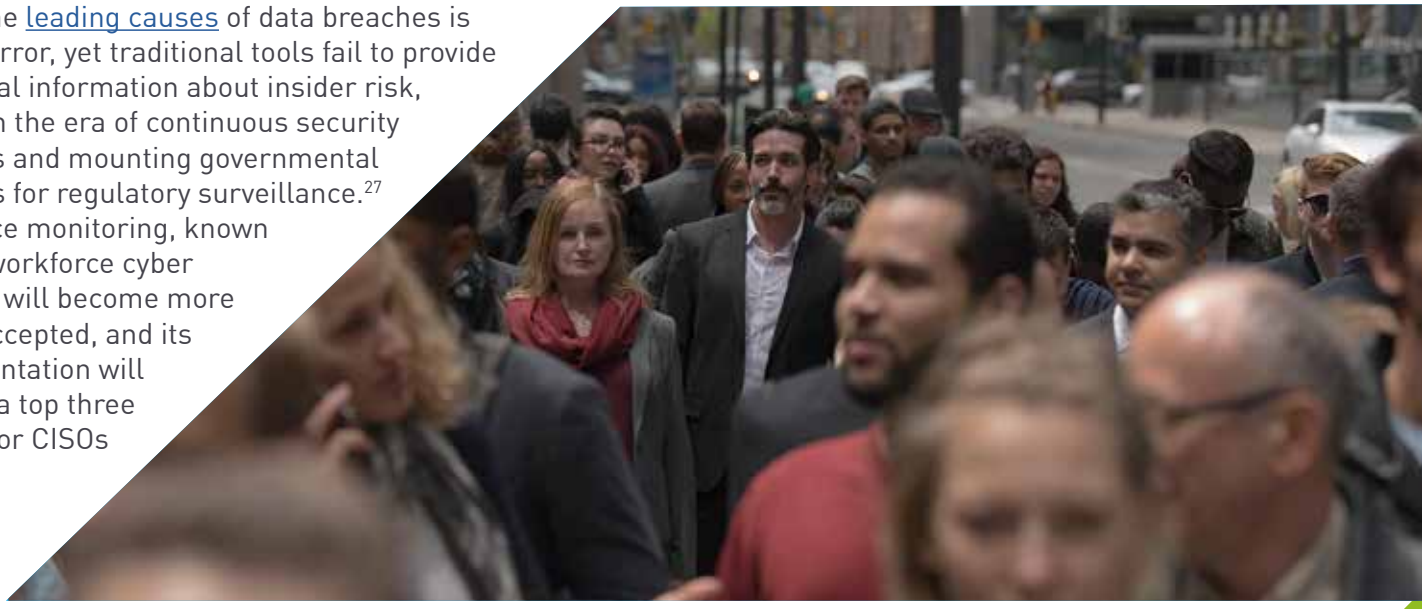
PREDICTION

An increasing amount of malware will become MITM-aware.

THE NEXT GIANT LEAP FOR THE INDUSTRY

Workforce monitoring moves from niche to necessary

One of the leading causes of data breaches is human error, yet traditional tools fail to provide contextual information about insider risk, critical in the era of continuous security breaches and mounting governmental demands for regulatory surveillance.[27] Workforce monitoring, known also as workforce cyber defense, will become more widely accepted, and its implementation will become a top three priority for CISOs in 2018.



"Organizations will realize that privacy requirements do not outweigh the need to monitor workforces, and so will look to UEBA tools to protect their data, livelihoods and profits."

GUY FILIPPELLI
VP OF SOLUTIONS,
DATA & INSIDER THREAT SECURITY

VISIBILITY INTO HUMAN RISK

The demand for organizations to understand cyber behaviors at the human point — the intersection of users, data and networks – is growing. Impersonating user behavior is difficult and it's easy to identify when a user's behavior pattern trends away from the normal. User Entity and Behavior Analytics (UEBA) tools integrate data sources, providing the ability to identify and prioritize high-risk activity within organizations, and detect potentially malicious and compromised user accounts.

Once inside a network, an attacker can act undisturbed. Since most insider threats aren't carried out using malicious code, traditional tools don't offer the required visibility. Organizations will adopt UEBA tools to create profiles based on their users' cyber behaviors, to gain visibility into human risk across the organization.

NON-TRADITIONAL DATA CONSUMPTION

Organizations will ultimately justify the monitoring of their workforces to enable them to protect their data, livelihoods and profits, increasing some tensions in the aforementioned battle between privacy and security. The emphasis will be on broadening the scope of user behavior analysis, and UEBA will incorporate previously untapped data streams such as real-time communications, public records, physical access patterns and potentially social media interactions on platforms like Twitter, Facebook and LinkedIn.

PREDICTION

Workforce monitoring and employing UEBA will be a top priority for CISOs in 2018.

CONCLUSION

Toward a human-centric future

There's no doubting the impact these predictions can have on the security industry. We know that traditional data leakage and ransomware will continue to be the focus for remediation and prevention, but we're watching closely as artificial intelligence and the IoT can also bring new risks in the near future.

Our predictions for 2018 showcase a myriad of challenges for those tasked with protecting people, data and networks. While each may involve a unique set of security technologies, there is not a single prediction that does not contain a human element, whether it be the need to preserve user privacy in the face of ever-increasing regulations or making sure our personal data, once aggregated, doesn't fall into the wrong hands.

Supporting growth targets and strategic initiatives will place extra pressure on IT teams, and might cause them to take shortcuts. If they give in to these pressures without applying the right technologies to security processes, the security and success of the entire enterprise could be put at risk. It is always a struggle to balance the right mix of resources between detection, mitigation and prevention. It's our view that you need to take a fluid approach and shift resources based on the current risk landscape.

After all, people and security are not a dichotomy; users have the potential to unintentionally compromise their own systems in one minute and be the source of innovation in the next, but only if we truly understand the human-centric root of risk.

LEARN ABOUT THE FORCEPOINT HUMAN POINT SYSTEM

www.forcepoint.com/humanpoint

REFERENCES

[1]Leonard, Carl. "Raytheon|Websense 2016 Security Predictions." Forcepoint, 2 Dec. 2015, blogs.forcepoint.com/security-labs/raytheonwebsense-2016-security-predictions.

[2]"Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016." Official Journal of the European Union, 4 May 2016, pp. 82–83., ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

[3]Moerel, Lokke. 130 Days, 1,500 Notifications: Does Dutch Breach Rule Foreshadow GDPR? The International Association of Privacy Professionals, 16 May 2016, iapp.org/news/a/130-days-1500-notifications-does-dutch-breach-rule-foreshadow-gdpr/.

[4]Gartner, Inc. (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. https://www.gartner.com/newsroom/id/3598917 [Accessed 2 Nov. 2017].

[5]Greenberg, Andy. "The Reaper Botnet Has Already Infected a Million Networks." Wired, Conde Nast, 20 Oct. 2017, www.wired.com/story/reaper-iot-botnet-infected-million-networks/.

[6]Millman, Rene. "IoT Malware Doubled in 2016, Says Report from Kaspersky." Internet of Business, 20 June 2017, internetofbusiness.com/iot-malware-doubled-2016/.

[7]Sage, Alexandria. "Ford Using First over-the-Air Software Updates to Its 2016 Cars." Reuters, Thomson Reuters, 19 May 2017, www.reuters.com/article/us-ford-motor-software/ford-using-first-over-the-air-software-updates-to-its-2016-cars-idUSKCN18F2BJ.

[8]Ward, Mark. "Smart Meters Can Be Hacked to Cut Power Bills." BBC News, BBC, 16 Oct. 2014, www.bbc.com/news/technology-29643276.

[9]Lopatin, Evgeny. "Miners on the Rise." Securelist, 12 Sept. 2017, securelist.com/miners-on-the-rise/81706/.

[10]Daian, Phil. "Analysis of the DAO Exploit." Hacking Distributed, 18 June 2016, hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/.

[11]Georgiev, Hristo. "The Hack That Changed the Blockchain Perspective." MWR Labs, 11 Aug. 2016, labs.mwrinfosecurity.com/blog/the-hack-that-changed-the-blockchain-perspective/.

[12]Baldwin, Clare. "Bitcoin Worth $72 Million Stolen from Bitfinex Exchange in Hong Kong." Reuters, Thomson Reuters, 3 Aug. 2016, www.reuters.com/article/us-bitfinex-hacked-hongkong/bitcoin-worth-72-million-stolen-from-bitfinex-exchange-in-hong-kong-idUSKCN10E0KP.

[13]Dela Paz, Roland. "Trickbot Goes After Cryptocurrency." Forcepoint Security Labs, 29 Aug. 2017, blogs.forcepoint.com/security-labs/trickbot-goes-after-cryptocurrency.

[14]Pressman, Aaron. "How 'Homeland' Fans Helped Hackers Mine Cryptocurrencies and Didn't Even Know It." Fortune, 26 Sept. 2017, fortune.com/2017/09/26/showtime-homeland-hack-cryptocurrency-monero/.

[15]Financial Services (Distributed Ledger Technology Providers) Regulations 2017, 2017. gibraltarlaws.gov.gi/articles/2017s204.pdf.

[16]Stolberg, Sheryl Gay. "Senate Passes $700 Billion Pentagon Bill, More Money Than Trump Sought." The New York Times, 18 Sept. 2017, www.nytimes.com/2017/09/18/us/politics/senate-pentagon-spending-bill.html.

[17]Chapman, Lizette, and Brad Stone. "The Worst Case Scenario After the Equifax Hack." Bloomberg.com, Bloomberg, 26 Sept. 2017, www.bloomberg.com/news/articles/2017-09-26/the-worst-case-scenario-after-the-equifax-hack.

[18]Riley, Michael, et al. "Equifax Suffered a Hack Almost Five Months Earlier Than the Date It Disclosed." Bloomberg.com, Bloomberg, 18 Sept. 2017, www.bloomberg.com/news/articles/2017-09-18/equifax-is-said-to-suffer-a-hack-earlier-than-the-date-disclosed.

[19]Weston, Liz. "Why banks want you to drop Mint, other 'aggregators'." Nov. 9, 2015, https://www.reuters.com/article/us-column-weston-banks/why-banks-want-you-to-drop-mint-other-aggregators-idUSKCN0SY2GC20151109.

[20]Nakashima, Ellen. "With a series of major hacks, China builds a database on Americans." June 5, 2015, https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html?utm_term=.30e367678529.

[21]Redmond, Tony. "Microsoft To Surpass 100 Million Office 365 Users in 2017." Petri, 24 Feb. 2017, www.petri.com/office-365-85-million-monthly-active-users.

[22]Bendor-Samuel, Peter. "How to Eliminate Enterprise Shadow IT." CIO, 11 Apr. 2017, www.cio.com/article/3188726/it-industry/how-to-eliminate-enterprise-shadow-it.html.

[23]Wall, Matthew. "Can We Trust Cloud Providers to Keep Our Data Safe?" BBC News, BBC, 29 Apr. 2016, www.bbc.com/news/business-36151754.

[24]HTTPS Encryption on the Web, transparencyreport.google.com/https/top-sites.

[25]Finley, Klint. "Half the Web Is Now Encrypted. That Makes Everyone Safer." Wired, Conde Nast, 3 June 2017, www.wired.com/2017/01/half-web-now-encrypted-makes-everyone-safer/.

[26]Griffin, Nicholas. "Japanese Banking Trojan 'Shifu' Distributed Via Malicious Word Documents." Forcepoint Security Labs, 11 Oct. 2015, blogs.forcepoint.com/security-labs/japanese-banking-trojan-shifu-distributed-malicious-word-documents.

[27]Bite, Blue. "Data Breaches: Leading Causes & How to Avoid Them – Blue Bite – Medium." Medium, Medium, 3 Apr. 2017, medium.com/@BlueBite/data-breaches-leading-causes-how-to-avoid-them-797e3d51b1b1.

ABOUT FORCEPOINT

Forcepoint is transforming cybersecurity by focusing on what matters most: understanding people's intent as they interact with critical data and intellectual property wherever it resides. Our uncompromising systems enable companies to empower employees with unobstructed access to confidential data while protecting intellectual property and simplifying compliance. Based in Austin, Texas, Forcepoint supports more than 20,000 organizations worldwide. For more about Forcepoint, visit www.forcepoint.com and follow us on Twitter at @ForcepointSec.

www.forcepoint.com/contact