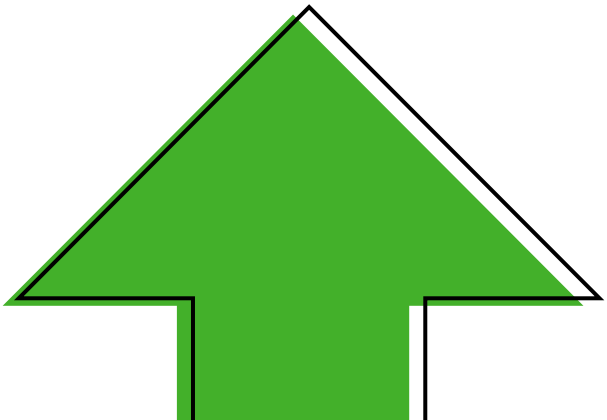
FORCEPOINT

POWERED BY Raytheon

2017 SECURITY PREDICTIONS

AN ANNUAL REPORT BY **FORCEPOINT** SECURITY LABS™

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Age of Convergence

Conventional thinking divides the digital and physical worlds into two distinct and separate realms. But is that still true?

In preparing this report, the persistent and compelling theme that kept surfacing as we identified our security predictions for 2017 was that of convergence. The integration of the digital and physical realms has reached a tipping point. We see the world transforming itself, blending both the digital and physical into a new and emerging world. From a cybersecurity perspective, convergence acknowledges the digital transformation process that is already well underway, how it affects us and how we, in turn, affect it.

Informed by our industry-leading experience in the security space and drawing upon the deep resources of both the Forcepoint™ Security Labs and Raytheon, we believe that security professionals are best served by viewing the digital and physical worlds as two halves of an integrating whole: although they both may remain *different*, they are no longer *separate*.

Our outlook in this report is intended to be as objective as possible, with a perspective defined not only by what we include, but also by what we do not. The essential message is that the world emerging before our eyes will challenge cybersecurity professionals in ways it never has before.

SECURITY PREDICTIONS FOR 2017

It's in this context of convergence that we present Forcepoint's Security Predictions for 2017:

1. The Digital Battlefield is the New Cold (or Hot?) War
2. Millennials in the Machine
3. Compliance & Data Protection Convergence
4. Rise of the Corporate-Incentivized Insider Threat
5. Technology Convergence & Security Consolidation 4.0
6. The Cloud as an Expanding Attack Vector
7. Voice-First Platforms and Command Sharing
8. AI and the Rise of Autonomous Machine Hacking
9. Ransomware Escalation
10. Abandonware Vulnerability

The order in which we present our security predictions generally falls into two categories:

Predictions 1-5 are macro events driven by larger forces, such as new developments in foreign policy, demographics, trade law, corporate policies and market forces.

Predictions 6-10 are positioned primarily in the digital realm. Some of our predictions overlap, lead into others or are closely related; but we believe that all of them have the potential for changing—and challenging—our world in 2017 and beyond.

01

THE DIGITAL BATTLEFIELD IS THE NEW COLD (OR HOT?) WAR

Cyber Attacks Are Now Seen as Acts of War

Under NATO Article 5, the new "Enhanced NATO Policy on Cyber Defense" allows for triggering a kinetic war in response to a hacking incident. The policy underscores that the continuing convergence of the cyber world with the real world has reached a precipitous level. In fact, the bridge between hacking and kinetic response has already been built and, at least to some degree, crossed:[2]

"...equating cyberspace with the other domains when talking about defense should mean that there is no longer a fundamental difference between them. The core assets of NATO in the other domains are capabilities with which it can defend itself, so now NATO should be prepared to develop these in cyberspace as well."[3]

NATO isn't the only military alliance or power to adopt this position. In fact, it's a response to the military cyber divisions China[4] and Russia[5] have had for years, even decades.

Rogue hackers may manipulate scenarios, triggering false flag cyber attacks misattributed to an innocent country.

As more countries are capable of carrying out disruptive or destructive cyber attacks to support political objectives, both offensive and defensive cyber operations and weapons strategy in peace and war time will become as important as physical weapons during actual conflict.[6]

Attribution remains a significant problem, with some cyber attackers state-sponsored and others, like ISIS, working independently of any government. Determining what constitutes an act of war without being able to assign ultimate responsibility for aggressions will complicate a unified international response.[7]

The rise of the "cyber terrorists" will prove to be a growing problem, and a potential target for military operations as enemies as the state.

02

MILLENNIALS IN THE MACHINE

Generational Employment Shifts Increase Cybersecurity Risks

Having grown up with the Internet and as early adopters of new technology, millennials bring an inherent openness to and trust of technology to the workplace that the retiring baby boomers never did. Now dominating the labor market, this first ever "digital generation" will have a significant impact on the workplace and, indeed, is already proving to be highly productive and innovative. Millennials' technological prowess and digital familiarity will certainly prove to be advantageous for employers, as millennials actively adopt new technology to improve their efficiency and job performance.[9]

Millennials represent a cultural shift that may prove challenging to workplace cybersecurity policies. They are accustomed to sharing their personal information and using their own digital devices, apps, etc. They also tend to have an elevated trust of technology and a tendency to embrace new connected devices that too often lack sufficient security to protect their data and privacy. Finally, with their multiple social media accounts, millennials present hackers an expanded attack surface.[10]

As millennials increasingly enter and change the cultural norms of the workplace, accidental data breaches may become more common.[11] Even as employers are adjusting some of their hiring practices and relaxing rules about accessing social media to accommodate millennial work habits, they are not addressing the security demands that come with those changes. Given their outdated technology and funding issues, federal agencies tend to be further behind the security curve than commercial employers. The key is for organizations to get ahead of the millennial security curve by adopting technology that puts context around employee behavior to distinguish between harmless or accidental behavior and risky or malicious employee activity.

03

COMPLIANCE & DATA PROTECTION CONVERGENCE

Data Protection Harmonization Becomes Law

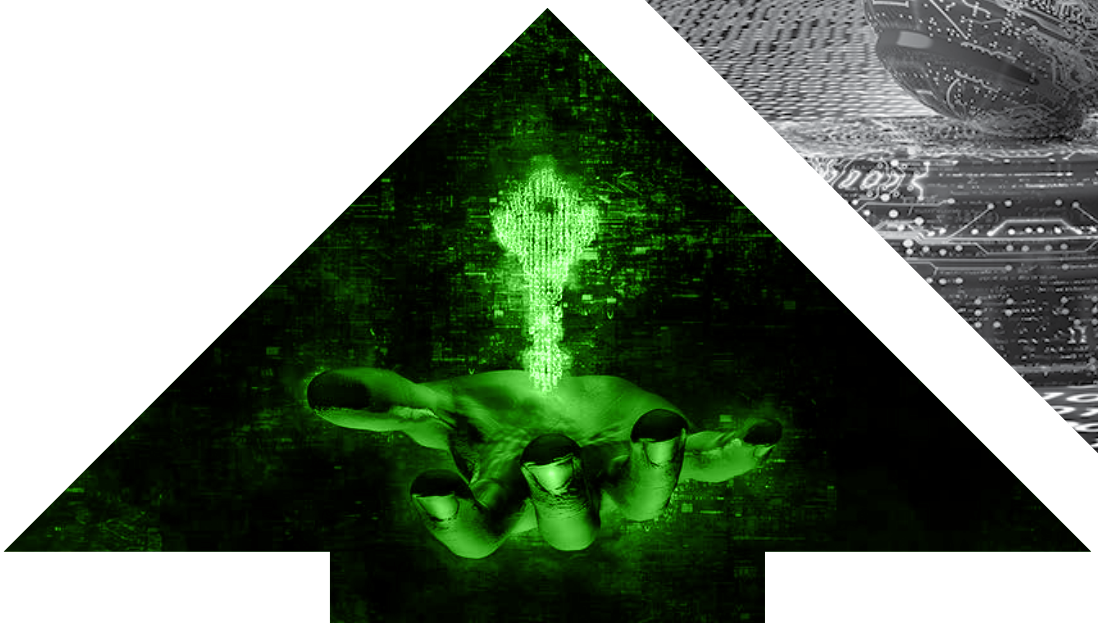
2017 will be the final full year before the European Union's (EU) General Data Protection Regulation (GDPR) is a legal requirement, with enforcement beginning in May of 2018.

Corporate and social responsibility for protecting personally identifiable information (PII) will converge and become a reality for organizations of all sizes. Many organizations will spend 2017 working with technology vendors to introduce new or updated technical controls in partnership with their internal teams as they move to dispose of old business processes that have no future in today's trust and privacy-first consumer world.

GDPR demands will drive business costs higher as new data protection controls are applied. Initially, fast data will be slowed as the convergence of data flows and analytics are re-examined. "Purpose," "consent" and "authorization" will be common terms used to define current and future business decisions on when and how multiple stakeholders across the business and the supply chain use data.

Risk registers will be *reset* and the new, true impact of a data breach may be re-examined prior to increased sanctions for non-compliance incidents beginning in 2018. The impact likely will be felt most by large enterprises that have not prepared in 2017.

Global managed service providers (MSPs) may be forced to increase costs. In-country analysts may be required and isolated technology instances will need to be deployed in order to separate customer data and ensure that only proper eyes can see it.



04

RISE OF THE CORPORATE-INCENTIVIZED INSIDER THREAT

Corporate Abuse of PII Expands

Recently, it was revealed that over 5,300 employees of a large bank used customers' personally identifiable information to open more than two million bogus accounts, generating millions of dollars in illegitimate fees to meet sales quotas. This is the result of the convergence of economic need for corporations to maximize profits and the opportunity for employees to meet sales quotas and keep their jobs by easy access to customer data and disguising their activities.

More cases of corporate-incentivized insider abuse of PII will come to light.[12] This may underscore a new definition of insider threat, where the organization inappropriately leverages their customers' data to meet corporate profit expectations and other performance goals. It won't be just from financial or banking institutions, either. The opportunity to generate revenue from taking advantage of millions—if not hundreds of millions—of customers' PII may prove to be too tempting for large organizations in other spaces to resist.[13]

Like the GDPR's new oversight, protections and access protocols may be proposed at the federal or even international level to further restrict both corporate and personal access to digital information, with far reaching legal and civil implications. Such proposals may follow in the wake of the Internet's transfer from American control to international governance.[14]

05

TECHNOLOGY CONVERGENCE & SECURITY CONSOLIDATION 4.0

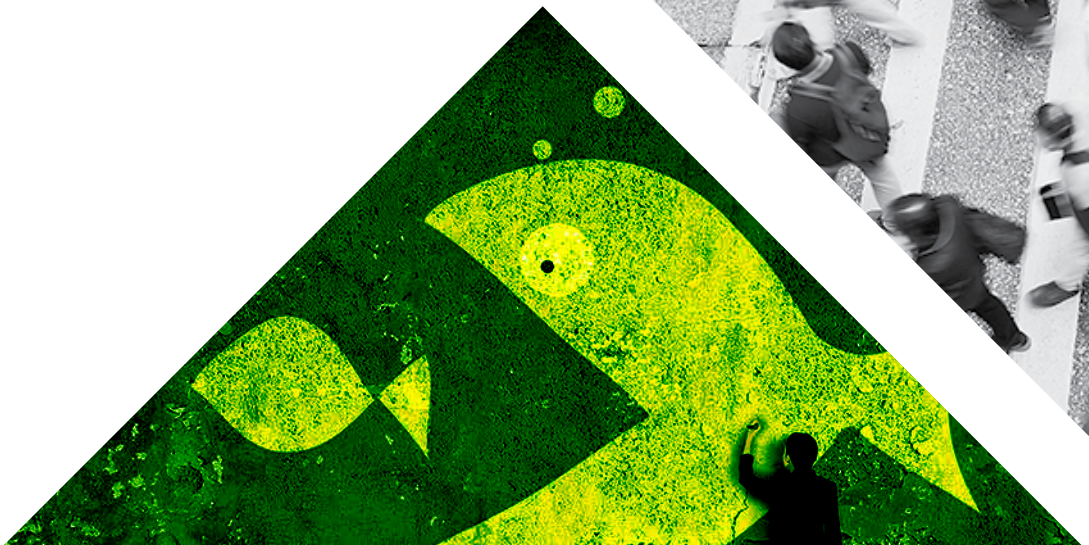
The High Impact of Market Forces

Cybersecurity corporations are now buying smaller security vendors, driving M&A consolidations.

As a result of vendor consolidation, those that are not a part of industry convergence or that aren't receiving additional venture capital will be more likely to exit the industry. We will see the beginnings of "dotbomb 2.0" emerge in this ever expanding and over populated industry.

We'll see more orphaned technologies, where owners stop supporting and upgrading their products, essentially abandoning them (also known as "abandonware"), and a temporary slowing of security technology innovation as the industry rides wave of consolidation. *(See Prediction 10: Abandonware Vulnerability - Cybersecurity's Achilles Heel? for the impact of abandonware vulnerabilities.)*

Security training and products focused on increasing security resources could be a next big wave to utilize the consolidated cybersecurity products.



06

THE CLOUD AS AN EXPANDING ATTACK VECTOR

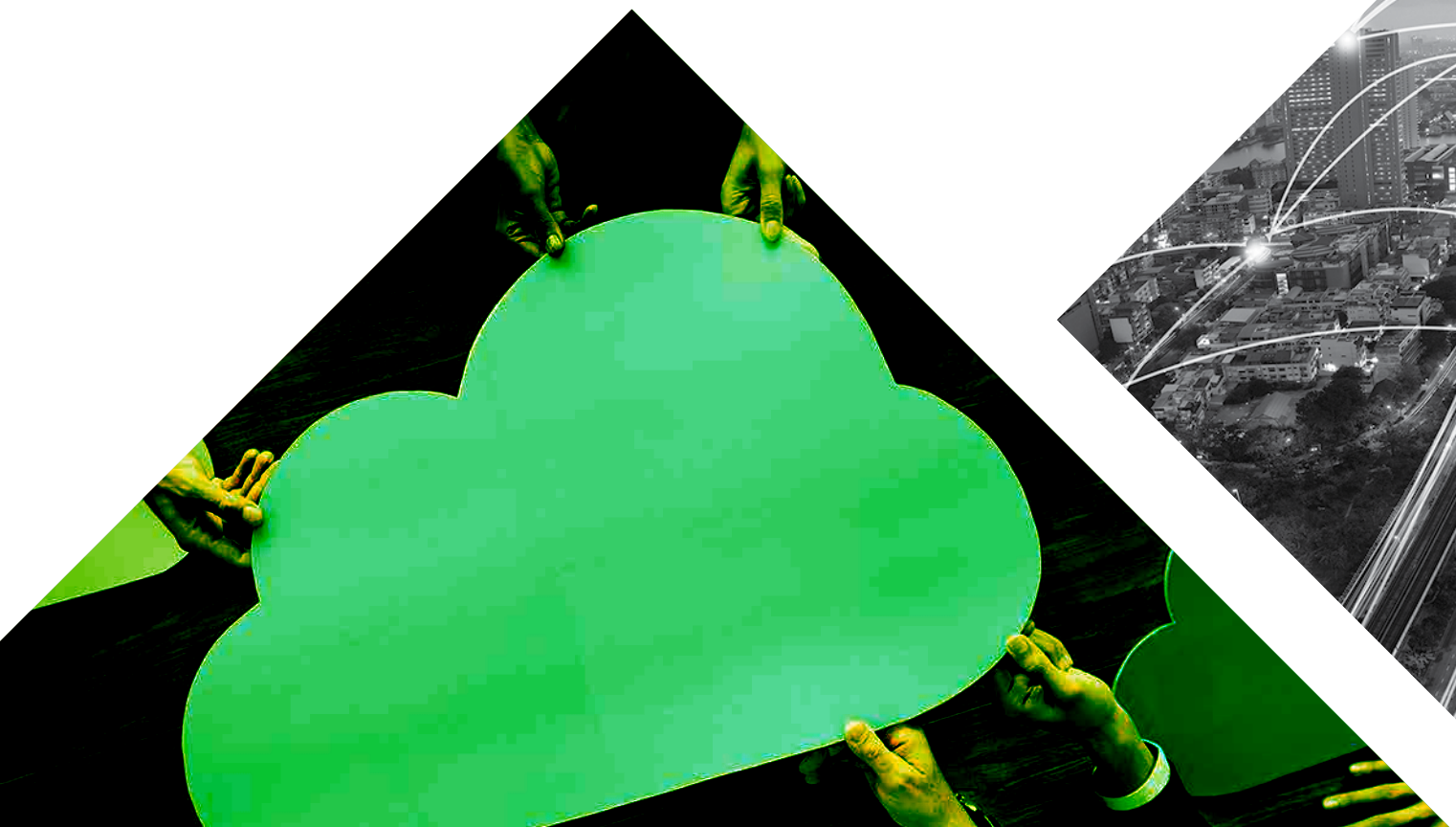
The Challenge to Securing Cloud Infrastructure

As migration to the Cloud rises, several new developments are putting users and data at risk in unintended ways.

The risk of hypervisor hacking may rise. With governments moving to the Cloud, the underlying foundation that runs virtual machines there may be increasingly subject to attack. If a hypervisor gets compromised attackers will have full control of any and all systems running there.

Organizations are migrating their already vulnerable environments to the Cloud, relying on it alone to provide expanded security reducing their security in the process and will look to hybrid security to protect their data wherever it is used or accessed.

Denial of Service attacks may rise against cloud providers. This will impact business against clients in an untargeted fashion, creating threats against businesses.



07

VOICE-FIRST PLATFORMS & COMMAND SHARING

A New Level of Human and Technology Convergence

Replacing traditional computer interaction with voice-activated AI means the ways in which we access the Web, data and apps will change. The emergence of voice-activated AI platforms such as Siri, Cortana and Amazon Echo that recognize and bond to devices, represents a new level of human and technology convergence. As the line between artificial and human intelligence blurs, machines will become more a part of human beings and the human experience.

AI assistants will alter user behavior and expectations from their Web experience, and ultimately, diminish users' autonomy. This will prove to be a sea change from one-to-one interaction between human and device that we have known thus far. Families and other groups may rely on one AI assistant as the central hub of the group's behavior, schedule and preferences. "Normal" human behavioral traits and expectations, such as personal and intimate privacy, will be challenged by the ever present eavesdropping of AI technology that interacts with—and knows — everyone in its presence.

The convergence of technologies will generate a new round of consolidation: The "big five" tech companies are all in the early stages of a race to wean us off of the graphical interface, the open Web, and the app ecosystem, and train us to use their respective AI assistants as our primary portal to the internet."[15]

The creators of AI interfaces will become powerful influencers of not just how we interact with machines, but also the slant of the information toward which the machines will be programmed to steer us. For example, which news channel will your AI interface, by default, send you to: CNN, BBC, RT or FNC?

The number of apps designed to leverage voice-activated AI such as Siri, Alexa and others, will explode in 2017, allowing a whole new threat vector to emerge. These new AI apps will gather ever more personal information on a vast number of users, providing new levels of convenience and an enhanced user experience. They may also pose unwanted risks, especially as regards access controls. New interface-based security risks will also accompany this app proliferation, allowing hackers to bypass existing security protection, leading to an increase in AI app-associated data breaches.

08

AI AND THE RISE OF AUTONOMOUS MACHINE HACKING

The Rise of Criminal Machines

Automated—and autonomous—hacking machines designed to rapidly seek out vulnerabilities and potential breaches in networks are here. The capabilities of AI cyber defense machines to search, surface, interpret and remediate attacks and potential breaches far outpaces human Security Operations (SecOps) teams' abilities.

Widespread weaponization of autonomous hacking machines by threat actors will emerge in 2017, creating an arms race to build autonomous patching.

Self-directed hacking machines may be launched by rogue hackers or state actors to anonymize attacks, target and overwhelm rival national cyber defenses, or to trigger a response that may quickly evolve into geopolitical and economic crises (*see Prediction 1: The Cyber Arms Race is the New Cold (or Hot?) War*). Like nuclear weapons technology proliferation, weaponized autonomous hacking machines may greatly impact global stability by either preventing national defense protocols being engaged or by triggering them unnecessarily.

09
RANSOMWARE ESCALATION

The Convergence of Hackers and Corporate Espionage

The huge success of ransomware in 2015 and 2016 likely means that we can expect more of the same in 2017. In the first half of 2016 alone, one gang of ransomware hackers made an estimated $121 million dollars.[16] There should be no expectation that ransomware will go away in 2017; as the saying goes, "Why mess with success?"

Why, indeed. The vast majority of organizations remain vulnerable to ransomware and, on average, 37% of the victims pay the ransom to re-obtain access to their critical data.[17] The number of exploit kits containing ransomware more than doubled from March through July in 2016 alone.[18]

Unethical organizations may fill their need for technological innovation and development by hiring ransomware hackers to obtain specific information from competitors. At the same time, ransomware hackers may offer to sell ransomed critical data to the highest bidders while collecting ransom payments from their victims. Why collect just one paycheck when you can collect two, or perhaps many more, from the same hack?

In order to accomplish the above, hackers will have to alter their current playbook, morphing ransomware to include data exfiltration techniques, to better capitalize on every ransomware hack.

10
ABANDONWARE VULNERABILITY

Cybersecurity's Achilles Heel?

Video gamers are not the only ones using post "end-of-life" products. For over a decade, IT security professionals and other security researchers have relied upon out-of-date, unsupported legacy tools to reverse engineer programs for a variety of purposes.[19] This trend shows no sign of reversing and is actually much more widespread than commonly known.

More than 75,000 users in the IT security field continue to use an abandoned or obscure software, unknowingly and unnecessarily putting themselves at risk.[20] We expect to see more legacy, end-of-life abandonware vulnerabilities leading to data breaches. This will occur both in the consumer and commercial spaces and, to the consternation of IT professionals everywhere, in the cybersecurity space as well.

Automated updates may also become a cause of security complacency among millions of users, significantly raising the risks of data breach. Most operating systems, including Microsoft®, Linux® and Apple OS X® distributions, as well as mobile devices such as Apple and Android tablets and phones, have automated updates or similar mechanisms. Others, such as Adobe Acrobat®, Flash Player®, Google Chrome™ and Firefox® browsers have their own internal update mechanisms. But with millions of users becoming familiar with and overly reliant upon these auto-updates to maintain sufficient anti-breach security in an increasingly sophisticated threat landscape.[21]

CONCLUSION

Achieving Security in Interesting Times

We are living in exceptionally dynamic times. The security challenges resulting from the rapid convergence of the digital and physical worlds aren't the only ones we will see, but we think they are certainly the most compelling. We believe that its progression will undoubtedly offer the world new advantages as well as some additional risks. Only by embracing the challenges we face in this new and emerging threat landscape can we develop solutions required to address them.

Our most important prediction, however, is a self-fulfilling one: At Forcepoint, we will continue to lead the industry in developing innovative products and solutions to meet the security challenges ahead, protecting organizations from cyber threats, wherever they originate and however they may manifest, today, tomorrow and on into the future.

CITATIONS

[1] Cyber defence [2016, July 27] NATO. http://www.nato.int/cps/en/natolive/topics_78170.htm

[2] Coker, Margaret in London, Yadron, Danny in San Francisco and Paletta, Damian in Washington. Julian E. Barnes in Brussels and Alexis Flynn in London contributed to this article. [2015, August 27] Hacker Killed by Drone Was Islamic State's 'Secret Weapon'. The Wall Street Journal. http://www.wsj.com/articles/hacker-killed-by-drone-was-secret-weapon-1440718560

[3] Minárik, Tomáš. [2016, July 21] NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit. CCDCOE. https://ccdcoe.org/nato-recognises-cyberspace-domain-operations-warsaw-summit.html

[4] Fadilpašić, Sead. [2015, March 19] China admits having cyber warfare divisions. ITProPortal. http://www.itproportal.com/2015/03/19/china-admits-cyber-warfare-divisions/

[5] Gady, Franz-Stefan. [2015, March 03] Russia Tops China as Principal Cyber Threat to US. The Diplomat. http://thediplomat.com/2015/03/russia-tops-china-as-principal-cyber-threat-to-us/

[6] Strategic Primer: 2016 Cybersecurity. [March 2016] American Foreign Policy Council. www.afpc.org/files/getContentPostAttachment/263

[7] Cheng, Joey. [2014, September 08] Raising the stakes: NATO says a cyber attack on one is an attack on all. Defense Systems. https://defensesystems.com/articles/2014/09/08/nato-cyber-attack-collective-response.aspx

[8] Fry, Richard. [2015, May 11] Millennials surpass Gen Xers as the largest generation in U.S. labor force. Pew Research Center. http://www.pewresearch.org/fact-tank/2015/05/11/millennials-surpass-gen-xers-as-the-largest-generation-in-u-s-labor-force/

[9] Millennial Myths vs. Reality: How to Engage and Hire Next Gen Talent. [2015, May 11] Human Resource Management Center. http://www.hrmc.com/white-papers/millennial-myths-vs-reality-how-to-engage-and-hire-next-gen-talent.aspx

[10] How Many Millennials, Gen Xers And Baby Boomers Use Facebook, Twitter And Instagram? [2014, June 03] Adweek. http://www.adweek.com/socialtimes/millennials-gen-x-baby-boomers-social-media/499110

[11] Millennial Rising "Digital Warriors" Introduce Risk to Federal IT Sysytems. [October 2016] LaunchTech. https://www.forcepoint.com/millennial-rising

[12] Dolmetsch, Chris and Campbell, Dakin. [2016, October 03] Morgan Stanley Unit Accused of High-Pressure Sales Tactics. Bloomberg. http://www.bloomberg.com/news/articles/2016-10-03/morgan-stanley-unit-accused-of-high-pressure-sales-tactics

[13] Kolhatkar, Sheelah. [2016, September 21] Elizabeth Warren and the Wells Fargo Scandal. The New Yorker. http://www.newyorker.com/business/currency/elizabeth-warren-and-the-wells-fargo-scam

[14] Moyer, Edward. [2016, October 01] US hands internet control to ICANN. CNET. https://www.cnet.com/news/us-internet-control-ted-cruz-free-speech-russia-china-internet-corporation-assigned-names-numbers/

[15] Oremus, Will. [2016, April 03] Terrifyingly Convenient. Slate. http://www.slate.com/articles/technology/cover_story/2016/04/alexa_cortana_and_siri_aren_t_novelties_anymore_they_re_our_terrifyingly.html

[16] A Single Ransomware Gang Made 121 Million In 2016. [2016, September 21] Active Technologies, LLC. http://active-technologies.com/content/single-ransomware-gang-made-121-million-2016

[17, 18] Sheridan, Kelly. [2016, August 03] Ransomware Hit Nearly 50% Of Businesses In 2015: Study. InformationWeek. http://www.informationweek.com/strategic-cio/security-and-risk-strategy/ransomware-hit-nearly-50--of-businesses-in-2015-study/d/d-id/1326491

[19, 20, 21] Freeman – The Perils of Abandonware. [October 2016] Forcepoint. https://blogs.forcepoint.com/security-labs/freeman-perils-abandonware

CONTACT

www.forcepoint.com/contact

FORCEPOINT
Security Labs™

For more information, visit: https://blogs.forcepoint.com/security-labs