STROZ FRIEDBERG
an Aon company

**ATTACKS INTENSIFY**

REGULATION EMERGES FROM THE SHADOWS

# 2017 CYBERSECURITY **PREDICTIONS**

**Published:** January 2017

# TABLE OF CONTENTS

## Intro



## 2017 Predictions



## Conclusion

**Preparing security professionals and business leaders for the most significant cyber threats in the coming year.**

# FOREWORD

## Welcome to Stroz Friedberg's Cybersecurity Predictions report.

> Last year, we shared a graphical commentary detailing our top six predictions for 2016. This year, with cybersecurity firmly entrenched as one of the most consequential issues impacting international security, politics, economic stability, and transactional crime, an understanding of existing and emerging cyber risks is more relevant than ever. This report draws on our experience in the field to help prepare security professionals and business leaders for the most significant cyber threats in the coming year.

**Reflecting back, most of our 2016 predictions – from cyber threats influencing the U.S. presidential election to Internet of Things (IoT) incidents shifting dialogue to security – for better or worse, were fulfilled.**

**We witnessed the power of hackers to wage an information war and influence public opinion,** when individuals allegedly associated with the Russian government penetrated the servers of the Democratic National Committee. Industry was awakened to the perils of unsecured IoT devices, following major attacks such as the October 2016 assault on Dyn[1]. Malicious and careless insiders also inflicted significant damage to organizations. In August 2016, UK-based accounting software firm Sage discovered that payroll details, including bank account and salary information, of more than 200 customer companies were leaked through the actions of an employee[2]. The FBI continues to investigate this year's SWIFT hack on the Bangladesh Central Bank in which suspects, believed to have been aided by a bank employee, stole $81 million[3].

While our prediction that cyber insurance prices would increase has yet to be statistically proven, 2016 witnessed a significant uptick in demand for cyber insurance, particularly in the wake of high-profile cases. Aon recently reported that, with approximately USD 1.7 billion in premium, **annual growth for cyber insurance coverage and product is running at 30 to 50 percent[4].**

Our 2016 prediction of a boardroom shuffle resulting in the appointment of cyber directors and dedicated risk committees did not materialize at the level we anticipated, and hoped. Nevertheless, the year did see regulators taking steps toward making cyber skills a requirement on the boards of public companies, and incentivizing boards to take more responsibility for directly overseeing cybersecurity. **Discussion around the Cybersecurity Disclosure Act[5]**, introduced in December 2015, is ongoing and in December 2016 New York State issued a set of revised cybersecurity regulations for financial services companies[6]. The first set of standards of its kind in the United States, the proposed regulations mandate the creation of a new job function, **require financial institutions to designate a Chief Information Security Officer (CISO), who will have principle reporting and oversight responsibilities for the company's cybersecurity program.**

# 2016 SCORECARD

| PREDICTION | SCORE | RESULTS |
|---|---|---|
| **Cyber threats influence the 2016 U.S. election** | **TRUE** | **Global cyber threats took center stage during the 2016 U.S. election.** Hackers associated with the Russian government penetrated the servers of the Democratic National Committee, exposing emails which influenced public opinion and even led to the resignation of the DNC chair. |
| **IoT incidents shift the dialogue from functionality to security** | **TRUE** | **New attacks on a bigger scale involving IoT ignited a conversation around the security connected consumer devices.** Cyber criminals harnessed IoT devices to launch major DDoS attacks, bringing down websites including Netflix, Spotify, Reddit, Amazon and others. |
| **Insider threat looms large** | **TRUE** | **Careless and malicious insiders caused significant damage in multiple high-profile incidents.** U.S. investigators announced that they suspected a bank employee had assisted attackers in the Bangladesh Bank SWIFT heist. |
| **Data processing and storage goes local** | **TRUE** | **Businesses started segregating cloud services and data centers geographically.** The agreement to implement the EU-U.S. Privacy Shield was agreed upon as a replacement for the EU-U.S. Safe Harbor rules. Uncertainty and political disputes continue around international data flows. |
| **Boardroom shuffle** | **MIXED** | **A growing number of public companies are seeking cyber-savvy board members, but this is still** far from a majority**.** Regulators moved to make boards take more responsibility and oversight for cybersecurity, introducing new proposals like those from the New York Department of Financial Services. |
| **Cyber insurance premiums skyrocket, regulators impose carrier 'stress tests'** | **MIXED** | **Demand for cyber insurance has skyrocketed, with Aon reporting annual growth for cyber insurance coverage and product running at 30 to 50 percent.** This demand is largely seen to be pushing up prices, but this has yet to be proven in figures. |

## 2017: The impending cyber landscape

We believe that the year 2017 will bring the intensification of longstanding trends that cybersecurity professionals today are vigilantly monitoring, while several new or enhanced challenges will present themselves in force. Further, threats already broadly recognized, such as the security risk inherently a part of IoT, social engineering as a criminal tactic of choice, and the ability of hackers to attack data and interrupt or compromise information sources, will intensify this year as exploit techniques become more cunning. This will in turn require companies to respond, in that the materialization of regulations and policy, the pressure to recruit and build best-in-class red teaming capabilities, and the necessity to accept that cybersecurity risk management is a critical part of doing business will influence companies across industries. And all the while we are of the view that, both globally and politically, nation state cyber espionage and information wars will continue to greatly influence elections and even policymaking, with Russia, China, Iran, and North Korea being regions of great concern.

**Looking at the predictions in totality, our theme for 2017 is the blurring of lines between the actions and responsibilities of the state, markets, businesses, and civil society.** In terms of risk, this looks like nation states adopting the 'whistleblowing' tactics of hacktivists, and criminals with relatively small resources being able to commit huge scale nation state-style attacks on banking systems or even critical infrastructure.

**We believe this nexus will be accompanied by strong movements in cybersecurity policy and regulation.** In some countries, this regulatory push will focus on increasing national security, in others, governments may use it to increase protectionism. As governments firm up their online regulatory regimes, we might see some positive effects, such as increased security innovation and public awareness. Mostly, however, we think that businesses will be burdened by the need to interpret what a fragmented global regulatory landscape means for their operations. Companies active in the United States will have to watch carefully as the newly-elected U.S. government and the pending administration define their position on the issue.

WE TRUST YOU WILL FIND THIS YEAR'S PREDICTIONS INSIGHTFUL AND USE THIS THINKING AS A LAUNCHING PAD TO ASSESS YOUR VULNERABILITIES, AND TAKE ACTION TO MITIGATE CYBER THREATS AND CHART A COURSE FORWARD.

# PREDICTIONS

# 1.

## Criminals harness IoT devices as botnets to attack infrastructure.

> In 2017 we will see IoT devices compromised, harnessed as botnets, and used as launching points for malware propagation, SPAM, DDoS attacks, and anonymizing malicious activities.

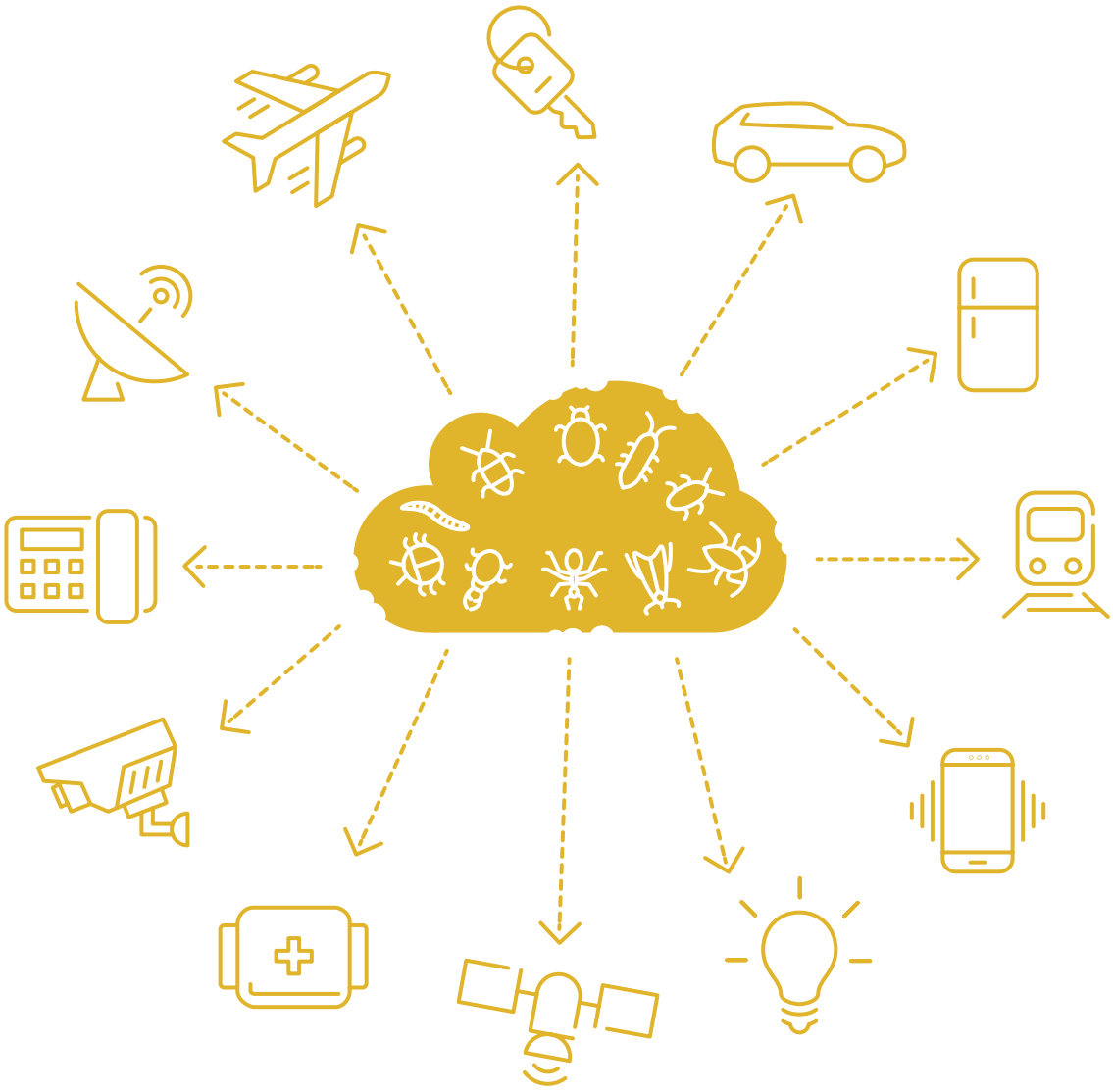
**As we predicted in last year's report, 2016 was the year criminal activity exposed the vulnerability of IoT devices.** The massive 2016 Distributed Denial of Service (DDoS) attack on internet infrastructure provider Dyn, caused by criminals infecting an army of unsecured IoT devices, including internet-connected DVRs, webcams, and cameras with malware, resulted in disruptions for access to major consumer websites including Twitter, Spotify, Amazon, and Netflix. The assault on Dyn[7] came shortly after the largest DDoS attack on record, launched from an IoT-enabled botnet of hacked devices, attempted to knock the security blog KrebsOnSecurity.com offline[8].

**This trend will intensify in 2017. Gartner predicts there will be nearly 26 billion internet-connect devices by 2020[9], and the smart home market alone is expected to reach $121.73 billion by 2022[10].** Verizon reported that IoT revenues were $217 million in Q3 of 2016, up 24 percent from the comparable period last year. With such a huge market opportunity and no baseline security regulations or standards in place for manufacturers, the number of everyday objects that present serious security risks will increase materially in 2017. At the same time, the number of DDoS attacks will grow— we've already witnessed rapid growth in 2016 with DDoS attacks increasing 71 percent in Q3 2016[11].

**Beyond DDoS attacks, this year we will also see a rise in ransomware attacks against the IoT, aimed at extorting more money and disrupting both business and consumer activity through connected devices.** In 2017, more U.S. employees will show up to work only to find their access to data blocked; patient files will be sealed in demand for payment, as in the 2016 Hollywood Presbyterian Medical Center attack[12]; and we predict an internet-connected hospital technology, such as an HVAC system, will likely be held hostage in demand for bitcoin payment. At the consumer level, a Nest system may demand part of a bitcoin for the homeowner to control the heat again and hobbyist drones will be found to be susceptible to remote control take-over, or used to conduct reconnaissance for a physical break-in.

**Despite calls from the security community for government regulation and set security standards to address the unprecedented risks posed by IoT devices, nothing significant has been issued.** To the chagrin of security practitioners and the delight of manufacturers, consumers have yet to realize that their seemingly innocuous devices could be a national security risk. There continues to be little financial incentive for conducting standard security assessments or integrating firewalls into IoT devices and manufacturers focused on getting products to market efficiently and profitably won't proactively drive improvements to security standards, or take the lead in integrating security into design. Many prominent consumer technology associations view consumer-led best practices, rather than government intervention, as the way forward.

*"Held hostage by your favorite device. In 2017, your Nest thermostat may demand a bitcoin to allow you to control the heat again."*



**BOTTOM LINE:**

While the conversation around IoT devices is beginning to switch from functionality to security, words have yet to be translated into actions. As long as this rapidly growing body of devices are unsecured, expect to see criminals exploiting them as an empowering platform from which to launch major attacks and they will often be directed at third parties. The fact that the IoT can be weaponized to attack third parties like Dyn and Krebs will lead to increased pressure for more responsible care over digital assets. As consumers wise up to these risks, their buying power could be a powerful voice in forcing manufacturers and government take the threat seriously.

# 2.

## Nation state cyber espionage and information war influences global politics and policy.

> Cyber espionage will continue to influence global politics and will spread to the upcoming elections in Latin America and Europe. Russia, China, Iran, and North Korea will be regions of great concern in 2017, as they continue to develop deep pools of cyber-crime talent. However, shifting internal politics and emerging U.S. foreign policy has the potential to influence this prediction.

**The 2016 U.S. election season was rocked by nation state-backed cyber attacks designed to obtain and release embarrassing information on political figures and party organizations, spreading suspicion and uncertainty among the public[13].** Politicians and political party leaders were stung by leaked email revelations and forced to respond to the fact they could no longer conduct negotiations and politics in the shadows. In response, in December 2016 U.S. President Barack Obama levied sanctions against nine entities and individuals over their alleged interference in the election. The administration also ordered 35 Russian diplomats to leave the country and two Russian compounds are being closed[14].

2017 will bring about more attacks from countries seeking to access and exploit sensitive information to realize their national interests, whether to wage an information war or conduct other destabilizing attacks such as disrupting networks or utility grids. **Cyber espionage and nation-state cyber warfare will escalate this year until it reaches a point that could be the cyber equivalent of the Cuban Missile Crisis.**

**With the decline in Chinese cyber espionage attacks on the United States, China will shift its efforts toward other countries, potentially Japan and South Korea.** South Korea, a world leader in Internet connectivity, with the world's fastest Internet connection speed and highest Internet penetration per capita (over 85 percent, while smart phone penetration rate is 80 percent), is a prime target[15]. It is also vulnerable – the country has already fallen victim to hacking of its financial institutions, stolen Korean Identification Numbers (KID), and malicious software disrupting government, public, and private networks and critical infrastructure.

**Russia, China, Iran, North Korea, and other countries with deep cyber-crime talent pools will continue to be the greatest concern in 2017.** Both China and North Korea organize training institutes for cyber hackers and cyber attack forces at the national level and possess highly advanced technology to launch cyber-attacks. These countries have developed information theft and other disruption activities that are used daily, penetrating the networks of government agencies and industries in Japan and the United States[16]. Russia's Ministry of Defense is establishing its own cyber command, which according to senior Russian military officials will be responsible for conducting offensive cyber activities, including propaganda operations and inserting malware into enemy command and control systems. Russia's armed forces are also establishing a specialized branch for computer network operations[17].

WITH THE UK AND OTHER COUNTRIES CLASSIFYING CYBER AS A TIER ONE THREAT – THE SAME LEVEL AS TERRORISM, OR INTERNATIONAL MILITARY CONFLICT - WE WILL ALSO SEE NATIONS TAKING STRONGER, DISCIPLINED RETALIATORY ACTIONS TO CYBER ESPIONAGE.

*"We will bear witness to an unprecedented and orchestrated cyber-espionage attack conducted by one nation on another."*

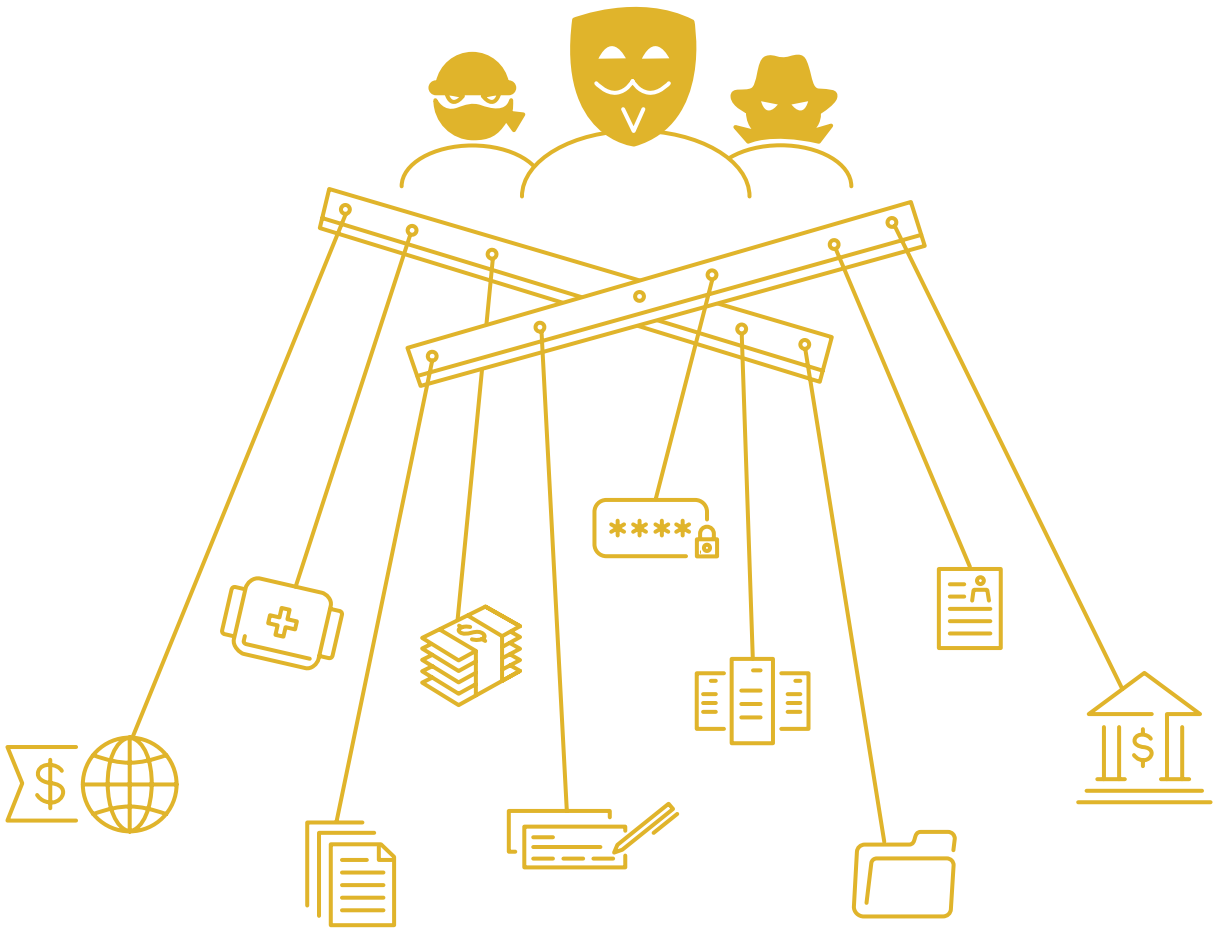
**BOTTOM LINE:**

In 2017, nation states will use cyber attacks to influence elections and policymaking in countries that do not share their political agendas. We will see a challenge to the status quo that taking down infrastructure on a huge scale requires the resources of one of these nation states. Expect highly skilled criminal groups that previously targeted the critical infrastructure of major regulated industries to move on to non-top tier targets with weaker defenses but equally valuable data, such as credit unions, less mature financial institutions, healthcare institutions, and manufacturing supply chains.

# 3.

## Data integrity attacks rise.

**Data sabotage as the next big threat will become a reality in 2017.** Criminals will seek to sow confusion and doubt over the accuracy and reliability of information, impairing decision-making across the private and public sector. Expect to see continued examples of governments or individuals reacting to altered or fake news articles as if they were true.



*"Criminals will successfully manipulate information, such as company earnings, news announcements, or the operational control of a system such as energy grids."*

**High profile attacks to date have already involved deleting data, editing news headlines, and disrupting access to information.** In November 2016, a group calling itself OurMine hacked Business Insider's website, posting and editing stories on the U.S. version of the website[18]. The U.S. election season was mired by the flood of "fake news" that independent researchers contend garnered support from a sophisticated Russian propaganda campaign that created and spread misleading articles online using botnets.

**In addition, data sabotage resulted in the December 2016 "PizzaGate" conspiracy[19].** This fake news story incited a man to open-fire in a pizza restaurant in Washington, D.C., claiming he was investigating a theory about Hillary Clinton running a child sex ring out of the establishment. Fortunately, nobody was injured. These incidences are just a foreshadowing of things to come. We are witnessing what James Clapper presented during his 2016 Congressional testimony as the "next push on the envelope."

IN 2017, IT WILL BE EVEN HARDER FOR INDIVIDUALS TO TRUST INFORMATION AND DATA, AND TO PROTECT IT FROM BEING ALTERED.

**Beyond news headlines, data integrity attacks will have even bigger ramifications.** Account executives might alter employee time sheet information before entering to the HR payroll application; altering of credit scores or bank account numbers will become more common, and is a natural evolution from simple data breaches; a corporate competitor who wants a competitive advantage might tamper with financial account databases to distort reality, immediately prior to a merger or closing of a significant contract.

**BOTTOM LINE:**

In 2017, organizations will prioritize protecting themselves against data integrity and sabotage after an incident in which criminals successfully manipulate information, such as company earnings, news announcements, voter information, or the operational controls of a system such as energy grids.

# 4.

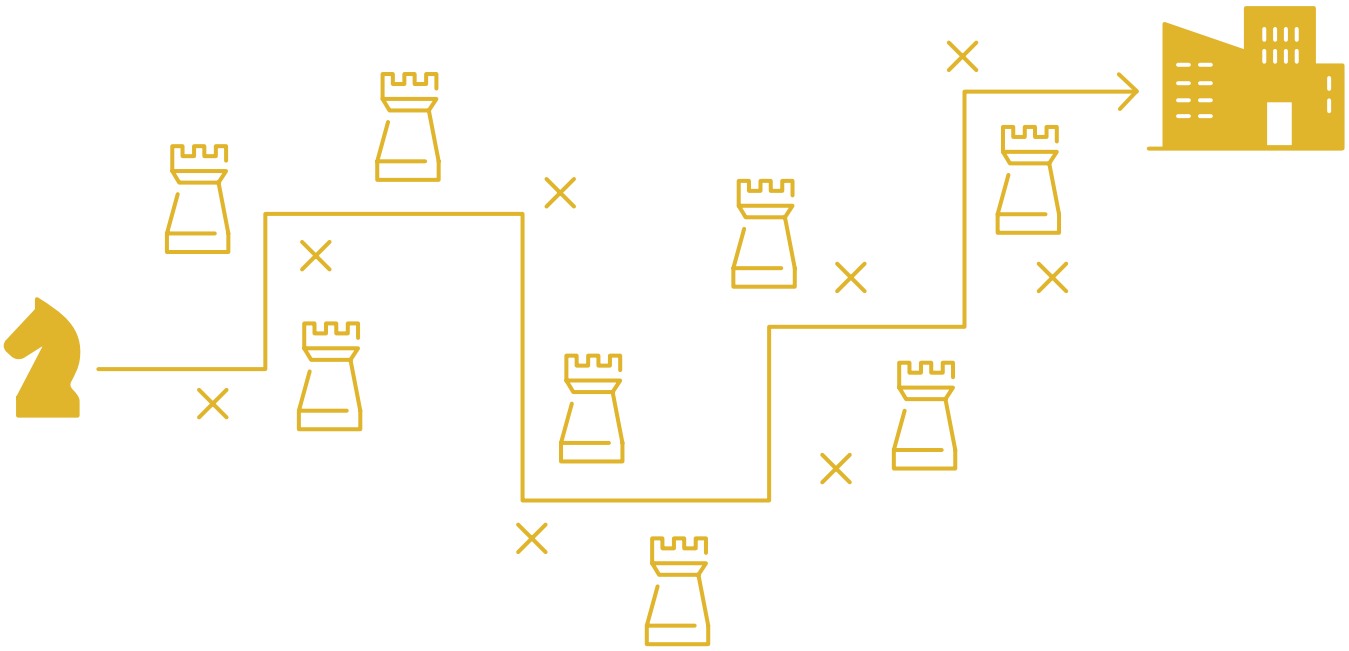
## Spear-phishing and social engineering tactics become more crafty, more targeted and more advanced.

As organizations continue to migrate to and embrace evolving technologies, including the cloud and IoT, and in parallel shore up perimeter defenses to raise the bar on network security, criminals will increase their focus on the human element as an entry point to pivot into broader network systems. In 2017, advanced social engineering tactics will become more targeted, cunning, and more effective, exploiting the weakest link – employees – that organizations always find challenging to safeguard.

**Defenses are improving around protecting infrastructure and new technologies that organizations are increasingly adopting, such as cloud services.** Providers like Amazon, Microsoft, and Google continue to bolster security to help protect companies that migrate their critical data to the cloud. As a result, in 2017 attackers will continue to increase their focus on targeting the human element, especially at the executive level of organizations. We will see an increase in spear-phishing attacks directed at insiders, third-party service providers, and business partners, aimed at gaining wider and faster access to data, such as information on a company's R&D, M&A activity, strategy, employee data, customers, and finance or other critical assets. The individual, device, and the interface in between the user and the cloud will become the primary targets for criminals hoping to obtain credentials. Therefore, employees will continue to be the Achilles heel of any security program and the critical line of defense against such attacks.

**Criminals will broaden the range of social engineering and phishing tactics they employ, including spear-phishing attacks, to increase their chances of success.** We will see cases of phishing tactics that will continue to be more authentic in appearance, with embedded malware that once clicked will infect or spread through an organization's system. We will also see an uptick in phishing scams targeting mobile devices, as well as social media sites that are accessed by employees on company mobile devices. Employees accessing social media at work has become part of routine business operations for most organizations, and the increasing reliance on accessing social media sites via mobile devices and apps, has created multiple security gaps ripe for exploitation by attackers. Adversaries will use more sophisticated coercion techniques to target employees, using knowledge gained from their social media profiles to extort them or exploit their human vulnerabilities to deceive them into providing sensitive information. To build a more robust profile of a target, criminals may even conduct a series of smaller attacks to gather personal information before launching one major attack to gain network credentials. In 2017, we expect to see adversaries hone in on "high value" targets, which no longer only means high net worth individuals or board members, but also those targets who can be used as entry points for access into systems and other critical assets, including heads of business units and employees in finance, operations, and HR departments.

**In 2017 attackers will build automation into their tools to more efficiently exploit credentials, company data, and sensitive information once credentials are obtained.** For example, once a set of credentials is discovered, they will be used in an automated fashion to gather more data - logging into other sites where the credentials work to collect more data and expand the dossier on the person to gain additional access. Security breaches of this nature are more likely to succeed in environments where there is negligence, carelessness, and lack of awareness regarding security and social engineering exploits.



**BOTTOM LINE:**

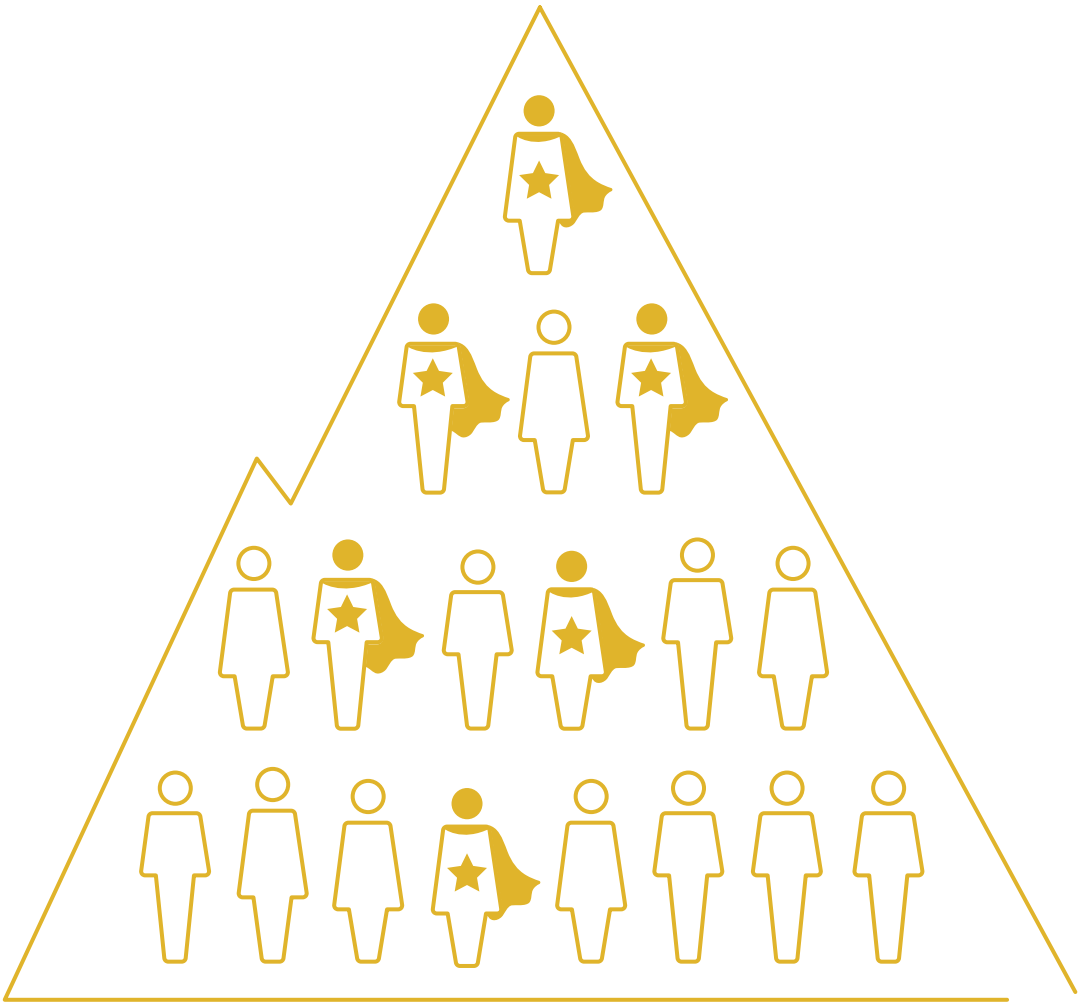
While the cloud, IoT, and other emerging technologies will continue to be leading data targets for hackers in 2017, attackers will increase their focus on the human element of technology along with other access points, including social media, building in automation to quickly exploit credentials, company data, and personal information. Increasing employee awareness and education, enforcing policies and implementing new technologies around employee behavior analytics to combat evolving and existing exploits will be essential.

*"Social engineering tactics will become more cunning – exploiting the weakest link in an organization."*

# 5.

## Regulatory pressures make red teaming the global gold standard with cybersecurity talent development recognized as a key challenge.

Increased pressure from regulators worldwide will push in-house red teaming capabilities to accelerate in 2017, and companies that are not in the cyber business will face a different challenge: recruiting, motivating, and retaining highly technical cyber talent to keep their red teams at the forefront of cybersecurity. This push will likely first occur in financial hubs such as Hong Kong, Singapore, the EU, and even the United States.



**In 2016, we predicted a boardroom shuffle in response to regulatory pressure.**

While policies and regulations continue to be discussed this year, we predict that red teaming will widely become the regulatory gold standard for the financial services industry, as it currently is in regions such as the UK. We also predict this will push adjacent industries that support financial services, such as telecommunications, to adopt this standard as best practice.

**Additionally, we expect this increased regulatory focus to drive and facilitate an uptick in companies creating in-house security capabilities beyond the financial sector, for example, in the critical infrastructure and healthcare industries.** Companies in sectors that already conduct adversarial testing in other areas, such as the energy sector assessing the vulnerability of their pipelines and other physical infrastructure, will conduct more cyber-focused red team testing. Outside regulated industries, first movers in sectors such as retail will tackle cyber risk with red teaming for the same reason – to understand their susceptibility to Advanced Persistent Threat (APT) actors.

**Specifically, the threat of large scale APT and nation state attacks on regulated sectors will spur regulators to explore mandating policies on intelligence-led testing frameworks much like the Bank of England's CBEST program.** Launched in the UK in 2015, the CBEST vulnerability testing program is designed to identify areas where organizations in the financial services sector could be vulnerable to sophisticated cyberattacks[20]. The model provides testing scenarios that are based on realistic situations, derived from current threat intelligence.

BUILDING RED TEAMING CAPABILITIES AND BEST PRACTICES WILL NOT COME WITHOUT CHALLENGES, HOWEVER, AS RESOURCE POOLS ARE SHALLOW FOR FRONTLINE PROTECTION.

**It is predicted that there will be a shortage of two million cybersecurity jobs worldwide this coming year.** While leading universities are introducing academic programs and scholarships to close this talent gap, classroom training in red teaming will not be enough. Even from military and intelligence training programs, the number of individuals trained in the area remains small, and the strongest red teamers have deep practical and technical experience in the field.

**As demand for these types of specialized security services increases, buyer organizations will need to be informed about the skills and expertise that a genuine provider should be equipped to offer.** They will need to be discerning as some providers attempt to market standard security assessments as red teaming products. The most valuable external providers will be able to offer outsourced red teaming services, and also share their expertise in setting up and supporting internal capabilities.

*"Regulatory pressures will make red teaming capabilities an industry gold standard"*

**BOTTOM LINE:**

In 2017, regulatory pressure on financial institutions to conduct red teaming will spark an uptick in the number of organizations across sectors establishing programs and bringing these capabilities in-house. To meet the demand for these skills, there will be a concerted effort to build new marketplace strategies and education programs to strengthen the talent pool. Companies will face pressure to retain talent as forward-thinking competitors will be aggressively seeking out security professionals with this skillset.

# 6.

## Industry first-movers embrace pre-M&A cybersecurity due diligence.

> The financial services industry will be the early-adopters of making cybersecurity due diligence a critical part of the pre-M&A due diligence process, learning from high profile transactions that were derailed in 2016 following the exposure of cyber vulnerabilities. While 2017 will see one to two additional high profile instances that impact the deal process outcome, only the financial services industry will react accordingly and conduct judicious cyber assessments.

CYBERSECURITY'S ABILITY TO IMPACT THE M&A PROCESS EXERTED GREAT INFLUENCE IN 2016, WITH MAJOR TRANSACTIONS DISRUPTED BY CYBER ATTACKS UNCOVERING VULNERABILITIES IN PRODUCTS OR AN ORGANIZATION'S DEFENSES.

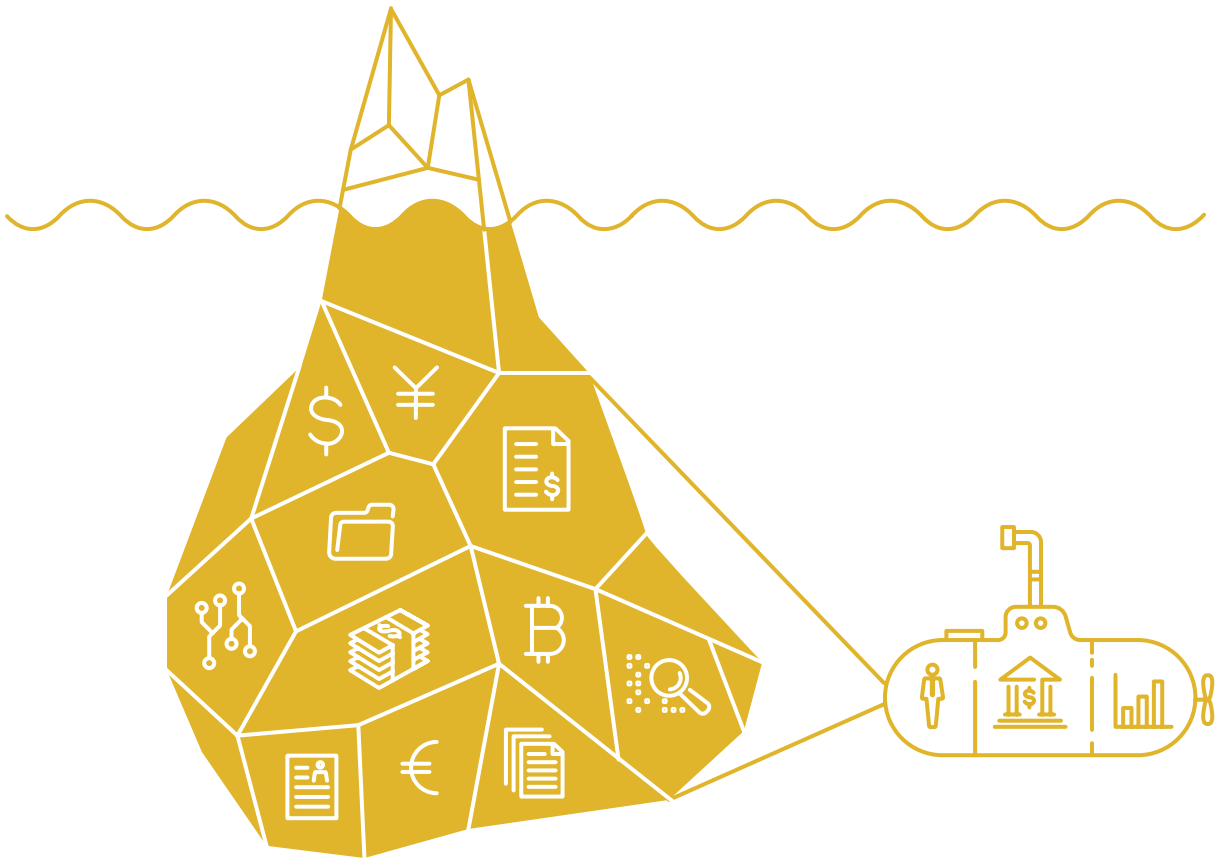
---

**In 2016, pharmaceutical company Abbott Laboratories' $5 billion deal to buy global medical device company St. Jude Medical was blackened by allegations of cybersecurity vulnerabilities in its products.** In August, a few months after St. Jude agreed to be purchased by Abbott, short-selling firm Muddy Waters announced its short position on St. Jude after receiving a report by cybersecurity firm MedSec claiming the company's cardiac devices are vulnerable to cyberattacks. Muddy Waters widely promoted its position and other notable short sellers began claiming that shares of St. Jude Medical could drop sharply if the takeover by Abbott Laboratories fell apart[21].

In 2017 we expect the financial services industry to adopt cutting-edge due diligence techniques such as searching the dark web for company data, seeing if employees are using their work email to set up online accounts, reviewing external facing intellectual property (IP) for evidence of persistent malware attacks, and talking to employees and former employees about how operations actually work with regard to information security.

**Acquiring companies will use these insights to assess the acquisition targets' cyber abilities and cybersecurity histories, and use the subsequent discoveries to adjust purchase price and terms.**

*"At least one high-profile transaction will be derailed due to the exposure of cyber vulnerabilities - or a cyber-attack - before industry will wise up to its M&A cyber due diligence responsibilities."*



**BOTTOM LINE:**

Financial services will continue to be the early adopter in understanding and mitigating the impact of connectivity on broader enterprise risk, shifting the emphasis of cybersecurity due diligence from post- to pre- M&A. Broadly, however, most organizations will not go into 2017 learning from 2016's M&A mistakes. It will take additional high profile deals to be impacted negatively by cybersecurity issues before cyber due diligence in pre-deal negotiations is taken seriously.

# CONCLUSION

**As government, business, and consumers balance rapid innovation in technology with changing cyber threats, every year sees an intensification of existing risks, and a number of new emerging ones. 2017 will be no different in that respect.**

What differs this year is the impetus and pending mandate to act. As stated in the foreword, governments worldwide, including the U.S. Trump administration simply due to their fear of nation state-style attacks, will begin to firm up online regulation and policies. With this, businesses in 2017 will be burdened by the need to interpret what a fragmented global regulatory landscape means for its operations.

**Nevertheless, industry is not powerless or relegated to sit by and wait for government directives to manage the risks we outlined in this paper. The below table presents concrete steps leaders can take today, in response to the substantial threat landscape, to shore up operations and boost defenses.**

WE INVITE YOU TO USE THIS REPORT AND RECOMMENDATIONS AS A LAUNCHING PAD TO ENGAGE IN DISCOURSE, ASSESS YOUR VULNERABILITIES, AND MOST IMPORTANTLY - TAKE ACTION TO MITIGATE THE THREAT LEVEL AND CHART A COURSE FORWARD.

| RECOMMENDATION | ACTIONS |
|---|---|
| **Optimize your cybersecurity posture. Continually assess and prioritize cyber threats and vulnerabilities, and improve incident response (IR) readiness.** | + Have an IR retainer in place to help minimize response times when an incident does occur.<br>+ Shift your mindset from conducting testing of a final version of a product to testing earlier in the development process. Conduct holistic testing, particularly when new technologies are introduced into an organization's ecosystems. Work with an outside provider on designing and implementing red teaming programs, and bringing them in house. |
| **Evaluate insider risk. Ensure your formal program is current.** | + Implement training and awareness around the current tactics and strategies that cyber criminals are using.<br>+ Conduct spear-phishing campaigns in your organization to help educate employees around what they should be looking out for. |
| **Conduct M&A pre-deal cyber due diligence early. Perform alongside compliance and financial due diligence.** | + Get your CISOs at the table early in the process. Provide adequate time to identify and remediate vulnerabilities in the cybersecurity posture and products of the company being acquired. |
| **Assess, protect and leverage intellectual property, and commercially valuable information.** | + Design and implement a strategy to proactively identify trade secrets, ensure the most effective protections are in place, and maximize the company's ability to respond rapidly and effectively when IP Is misappropriated or infringed. |
| **Consider self-regulation by adopting higher security standards in products and services prior to going to market, even if cost is prohibitive.** | + It's no longer just the role of government or law enforcement to stop cyber criminals— since networked technology can be weaponized and used against individuals and third parties. It's in a business's best interest to be a good corporate citizen. |

# CONTACTS


UNITED STATES

**Edward Stroz**
*Co-President*
E: estroz@strozfriedberg.com
T: +1 212 981 6541

**Rocco Grillo**
*Cyber Resilience Leader*
E: rgrillo@strozfriedberg.com
T: +1 212 981 2674

**Andrew Nairn**
*Co-Founder, Gotham Digital Science*
E: andrew@gdssecurity.com
T: +1 917 755 7519

**Carolyn Vadino**
*Chief Communications Officer and Marketing Leader*
E: cvadino@strozfriedberg.com
T: +1 646 524 8454

UNITED KINGDOM

**Eli Jellenc**
*Vice President, Threat Intelligence*
E: ejellenc@strozfriedberg.co.uk
T: +44 20 7061 2244

**Justin Clarke-Salt**
*Co-Founder, Gotham Digital Science*
E: justin@gdssecurity.com
T: +44 330 660 0720

# REFERENCES


1. Dyn.com, Dyn Statement on 10/21/2016 DDoS Attack, October 22, 2016 http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
2. Financial Times, Sage Hack Highlights Wider UK Data Struggle, August 26, 2016. https://www.ft.com/content/9b8386f4-687e-11e6-a0b1-d87a9fea034f
3. Wall Street Journal, FBI Suspects Insider Involvement in $81 Million Bangladesh Bank Heist, https://www.ft.com/content/9b8386f4-687e-11e6-a0b1-d87a9fea034f
4. Aon Benfield, Reinsurance Market Outlook, September 2016. http://thoughtleadership.aonbenfield.com/documents/20160911-ab-analytics-rmo.pdf
5. Congress.gov, Cybersecurity Disclosure Act of 2015, December 17, 2015. https://www.congress.gov/bill/114th-congress/senate-bill/2410/text
6. NYS DFS Regulations: http://www.dfs.ny.gov/legal/regulations/proposed/rp500t.pdf
7. Dyn.com, Dyn Statement on 10/21/2016 DDoS Attack, October 22, 2016 http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack/
8. KrebsonSecurity.com, KrebsonSecurity hit with Record DDoS, September 2016 https://krebsonsecurity.com/2016/09/krebson-security-hit-with-record-ddos/
9. Gartner, "Forecast: The Internet of Things, Worldwide, 2013," December 12, 2013. https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-
10. Markets and Markets, "Smart Home Market by Product Report," May 2016. http://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html?gclid=CNrckM6Gq9ACFUgbaQodA-8gEVQ-
11. Akamai Technologies' third quarter 2016 State of the Internet/Security Report. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q3-2016-state-of-the-internet-security-report.pdf
12. LA Times, Hollywood hospital pays $17,000 in bitcoin to hackers; FBI investigating, February 16, 2016. http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html
13. Wall Street Journal, Russian Hackers and American hacks, December 12, 2016. http://www.wsj.com/articles/russian-hackers-and-american-hacks-1481499091
14. CNN, White House announces retaliation against Russia: Sanctions, ejecting diplomats, December 30, 2016 http://edition.cnn.com/2016/12/29/politics/russia-sanctions-announced-by-white-house/index.html?adkey=bn
15. United States Dept. of State, Bureau of Diplomatic Security, OSAC, "South Korea 2016 Crime and Safety Report," April 2016. https://www.osac.gov/pages/ContentReportDetails.aspx?cid=19449
16. The Georgetown Journal of International Affairs, Nitta, Dr. Yoko, "Cyber Intelligence: The Challenge for Japan," March 17, 2015. http://journal.georgetown.edu/cyber-intelligence-the-challenge-for-japan/
17. House Permanent Select Committee on Intelligence, James Clapper, "Statement for the Record: Worldwide Cyber Threats," Sept. 10, 2015. https://www.dni.gov/index.php/newsroom/testimonies/209-congressional-testimonies-2015/1251-dni-clapper-statement-for-the-record,-worldwide-cyber-threats-before-the-house-permanent-select-committee-on-intelligence
18. Business Insider, Business Insider was hacked. November 2, 2016. http://www.businessinsider.com/business-insider-hacked-by-ourmine-passwords-reused-2016-11
19. The New York Times, Aisch, Gregor, "Dissecting the #PizzaGate Conspiracy Theories". December 10, 2016. http://www.nytimes.com/interactive/2016/12/10/business/media/pizzagate.html
20. Bank of England, CBEST Vulnerability Testing Framework Launch. http://www.bankofengland.co.uk/financialstability/fsc/Pages/cbest.aspx
21. CNBC, Fox, Michelle, "Muddy Waters' Carson Block says St. Jude Medica shares could fall to $55," August 26, 2016. http://data.cnbc.com/quotes/STJ

## ABOUT STROZ FRIEDBERG

Stroz Friedberg, an Aon company, is a specialized risk management firm built to help clients solve the complex challenges prevalent in today's digital, connected, and regulated business world. A global leader in the fields of cybersecurity, with leading experts in digital forensics, incident response, and security science; investigation; eDiscovery; and due diligence, Stroz Friedberg works to maximize the health of an organization, ensuring its longevity, protection, and resilience. Founded in 2000 and acquired by Aon in 2016, Stroz Friedberg has thirteen offices across nine U.S. cities, London, Zurich, Dubai, and Hong Kong, Stroz Friedberg serves Fortune 100 companies, 80% of the AmLaw 100, and the Top 20 UK law firms. Learn more at https://www.strozfriedberg.com/.

STROZ FRIEDBERG
an Aon company