2018 Cyber Predictions: Reality Check
Using Real Time Insights to Deliver Better Protection

Published: October 2018
Table of Contents

Introduction

Foreword ................................................................. 1
Prediction 1: Waking up to cyber liability ......................... 2
Prediction 2: Managing cyber as an enterprise risk ............. 3
Prediction 3: Regulatory spotlight widens .......................... 4
Prediction 4: Criminals attack businesses embracing IoT ....... 5
Prediction 5: Companies implement multi-factor authentication 6
Prediction 6: Bug bounty programs go mainstream ............... 7
Prediction 7: Ransomware attackers get targeted ................. 8
Prediction 8: Insider attacks fly under the radar ................. 9

Summary ........................................................................ 10

Contacts ................................................................. 11
2018 Cyber Predictions: Reality Check

Using Real Time Insights to Deliver Better Protection

In 2018, cyber risk has advanced. With growing Internet of Things (IoT) botnets, ransomware that targets backups, and an increasingly complex regulatory environment—cyber risk management must keep up. The goals stay the same: to protect business continuity and your organization’s information. But what needs to be done to achieve these goals changes as rapidly as do the threats.

To help clients and the broader enterprise community stay a step ahead of the newest tactics of cyber attackers, Aon’s Cyber Solutions offers annual predictions each January. These forecasts come straight from our elite force of incident responders, proactive security advisors, cybersecurity testing technicians, and cyber insurance leaders—based on their first-hand experiences in the field, working with boards and C-Suites across multiple industries and company sizes.

Now it’s 10 months later. A lot has changed. Some of it we predicted. Some of it we didn’t. What is important is for you to know how to protect your business going forward. October is National Cybersecurity Awareness Month and we’re updating our 2018 predictions with what has really happened over the course of the year. On top of that, we’ve added recommendations of techniques and strategies to help you better manage the risks. Read on to learn more.
Prediction 1. Businesses adopt standalone cyber insurance policies as boards and executives wake up to cyber liability.

REALITY CHECK
Businesses continue to adopt cyber insurance policies, as Aon has seen cyber insurance sales grow in excess of 25% year over year.

Three factors have driven this growth. First, as we predicted, boards and executives have become acutely aware of the potential for financial loss arising out of a cyber attack. The major ransomware attacks from 2017 were a wake-up call. Throughout 2018, for example, businesses have still been reporting losses from the NotPetya attack. To date, enterprises have seen minimum financial loss and extra expense estimates of USD 2.2 billion per public filings.

Second, some of these financial losses stemmed from business’ inability to operate as a result of the attack. As a result, executives are looking for insurance solutions to help solve cyber-driven business continuity risk.

Third, insurance carriers have been reviewing cyber coverage extensions under property and casualty policies with increased scrutiny, just as executives have begun to want affirmative protections for damages caused by cyber attacks. Executives have been looking for insurance solutions that address cyber risks, whether under a property or casualty policy, or a standalone cyber insurance policy.

Recommendation:
You should continually review your portfolio of insurance programs. Cyber insurance is rapidly evolving as risks and exposures do, too.
**Prediction 2.** As the physical and cyber worlds collide, chief risk officers take center stage to manage cyber as an enterprise risk.

---

**Recommendation:**
Quantify, quantify, quantify. Only when you know the financial damage that a risk can cause, can you understand how to mitigate it strategically and proportionally. Without this information, you’re battling risk with assumptions.

---

**REALITY CHECK**
Stakeholders across organizations are becoming better aligned to address cyber risk as an enterprise risk. One result is a new level of attention on cyber risk quantification.

As cyber risk becomes treated more like an enterprise risk, traditional risk management practices such as quantification are being applied. Cyber risk quantification helps organizations understand the maximum financial impact of cyber-related financial loss, and then prioritize and plan risk reduction and transfer strategies appropriately.
**Prediction 3.** Regulatory spotlight widens and becomes more complex, provoked calls for harmonization. The EU holds global company to account over GDPR violation; big data aggregators come under scrutiny in the US.

**REALITY CHECK**

No global company has been held accountable (yet) for GDPR violations, but data privacy and cybersecurity regulations are an increasing challenge for most organizations, as they become more numerous and complex.

The GDPR has encouraged U.S. states such as California to pass similar privacy regulations, raising the question if other U.S. states will follow suit. Recently Vermont passed the United States’ first law regulating data brokers. At the federal level, the Social Media Privacy Act of 2018 was introduced to the Senate. In February 2018, the Securities and Exchange Commission issued guidance to public companies for disclosing cybersecurity risks and incidents, emphasizing the breadth of corporate liability. Following this guidance, the SEC fined a major internet company millions of dollars for failing to disclose a breach.

**Recommendation:**

Rely on people who specialize in data privacy and cybersecurity regulations to help you navigate this legal labyrinth. Aon can help by assisting with the management of financial and regulatory risks associated with processing personal data under the GDPR.
Prediction 4. Criminals look to attack businesses embracing the IoT, in particular targeting a small to mid-sized company providing services to a global organization.

REALITY CHECK
Small-to-midsized IoT providers are being targeted to impact major organizations. Additionally, giant IoT botnets are being created.

This year, much of the Internet of Things (IoT) in large enterprises has been sourced from small-to-medium sized businesses (SMB), and has been managed remotely by the SMB through open doors in the larger corporation’s network—a practice that contributes to increased risk. Aon has been proactively and reactively working with manufacturing and energy multinationals to help reduce their IoT-related risk and respond to attempted attacks. These industries face particularly severe risks, as their IoT devices are large-scale, industrial control machines, for which they too rely on remote SMBs to manage.

The risk is high, however, across many sectors. In March 2018, the Ponemon Institute described the management of third party risks as “herculean” given the proliferation of IoT devices in its “Second Annual Study on The Internet of Things (IoT): A New Era of Third-Party Risk.” IoT devices are notoriously unsecured, and proper patch management programs have continued to be overlooked. As a result IoT botnet armies like The Hide ‘N Seek IoT botnet with more than 90,000 devices have been created, and cybersecurity experts are waiting to see what they will be used for.

Recommendation:
Consider testing the security of IoT applications by performing hardware security assessments, embedded security penetration tests, and firmware analysis, as well as risk assessments, security architecture assessments, and network security reviews.

1 https://www.securityweek.com/hide-n-seek-iot-botnet-can-infect-database-servers
REALITY CHECK

Multifactor authentication (MFA) is more important than ever before. Fallibility of physical biometrics and passwords aside, Aon sees the lack of MFA as a high-risk vulnerability.

While there are many vulnerabilities that contribute to becoming the victim of cyber attacks, not having MFA enabled is a major one. This year, many of the attacks Aon responded to happened at companies that didn’t adequately implement MFA. All this said, MFA adoption is on the uptick. Victim companies are quick to adopt it, and during our security assessments and reviews, we are seeing many more companies using MFA. There’s also another trend driving adoption. As more enterprises use Security Assertion Markup Language (SAML) based Single Sign-On (SSO), which allows an employee to use their company login for multiple cloud and on-premise services, MFA use is growing because most of these services have MFA.

Prediction 5. As passwords continue to be hacked, and attackers circumvent physical biometrics, multi-factor authentication becomes more important than ever before.

Recommendation:
Change management issues may inhibit the adoption of MFA at large corporations, but you should weigh the inconveniences of adoption through cyber risk quantifications to help decide how to proceed.
Prediction 6. Criminals will target transactions that use points as currency, spurring mainstream adoption of bug bounty programs.

**REALITY CHECK**

Bug bounty programs have become mainstream for mature organizations, though not because of risks in points programs. However, the effectiveness of bug bounties is getting questioned.

As of June this year, more than $31 million has been awarded to security researchers via bug bounty programs, up from just $11.7 million in all of 2017, according to HackerOne’s “Hacker-Powered Security Report 2018.” Anecdotally during the year, a major automotive organization advanced its bug bounty program; a technology products company announced a bug bounty program for its devices; and a software company created a new program focused on identity services.

However, there have been weaknesses identified in these programs. Bug bounty programs are structured to focus on high severity vulnerabilities that if exploited would have a direct impact on the business. As a result, lower risk findings can be missed—and these lower risk findings can be consequential.

**Recommendation:**

Traditional network, application, and IoT device penetration testing, which is more comprehensive and in-depth, is still recommended widely—even for companies with bug bounty programs.
Prediction 7. Ransomware attackers get targeted; cryptocurrencies help ransomware industry flourish.

REality CHECK
Ransomware is getting more targeted, and insidious—even encrypting backup files. Cryptocurrencies are helping the industry flourish.

Ransomware attacks are getting more strategic. This year, Aon has seen ransomware target companies being acquired because hackers believe they will pay up to avoid reporting the incident to their new parent companies. With the Crysis variant of ransomware, attackers are asking wealthier companies for more money than smaller firms—a trend likely to accelerate. Attackers have also been going after administrative credentials through a popular ransomware variant called SamSam. To further complicate the issue, some attackers are now encrypting backup servers as well, meaning the victim organization would have needed offline backups to outwit the attack.

Cryptocurrencies are continuing to help the industry flourish, particularly Monero (XMR) which is less easily tracked than other cryptocurrencies. Additionally, organizations are becoming victims of cryptomining attacks, where attackers steal organization’s processing power to earn cryptocurrency.

Recommendation:
Companies should regularly perform cyber-attack simulations as well as incident response readiness assessments focused on the newest ransomware trends. Companies should also consider cyber insurance coverage, as it offers cover not only for the ransom, but also for certain associated forensic consulting and business disruption expenses.

2 https://blog.barkly.com/what-is-samsam-ransomware-2018
**Prediction 8.** Insider risks plague organizations as they underestimate their critical vulnerability and liability, and major attacks continue to fly under the radar.

---

**REALITY CHECK**
Aon’s cybersecurity team is seeing an increase in insider attacks and an increase in risk because of Bring Your Own Device (BYOD) policies, cloud use, and visibility into data type.

Insider risk is increasingly challenging to manage as BYOD has extended from smartphones to laptops. When employees use their own laptops, they retain local administrative rights and companies often struggle to control information flow on these machines. As cloud use has expanded, organizations are often not monitoring files as they move from corporate to personal accounts.

Another complication to insider risk management is intent and visibility into data type. When data loss protection tools signal that files have been moved, it could just be an employee copying their photos and personal files, or it could be a policy violation, but not necessarily a trigger for litigation. Without knowing, an organization must decide whether to invest in an investigation.

---

**Recommendation:**
Organizations looking to enhance protections against insider risk should consider security operation center optimization, enhanced monitoring, and an incident response retainer, because these measures encourage organizations to investigate the intent of data transfers.
Information sharing is a key tenet of cyber risk management. Threats evolve rapidly as do the protections available and risk mitigation best practices. At Aon’s Cyber Solutions, we use our experience to help our clients understand which approaches are effective and what to consider when addressing cyber as an enterprise risk. We hope this access into the first-hand experiences of our elite cyber leaders helps you continue to solve against this ever-advancing risk.
Contacts

**United States**

**Rocco Grillo**
Cyber Consulting Leader—Cyber Solutions
Aon
rocco.grillo@aon.com
+1.212.981.2674

**Chad Pinson**
Executive Vice-President—Engagement Management—Cyber Solutions
Aon
chad.pinson@aon.com
1+214.377.4553

**Jay Stampfl**
National Sales Leader—Cyber Solutions
jay.stampfl@aon.com
1+ 203.682.6470

**United Kingdom**

**Justin Clarke-Salt**
Managing Director, EMEA—Cyber Solutions
justin.clarke-salt@aon.co.uk
+44 330 660 0720

**Alex Carte**
Managing Director, Cyber Practice Leader M&A EMEA—Cyber Solutions
Aon
alexander.carle@aon.co.uk
+44 20.7061.2302

---

**Jason J. Hogg**
CEO—Cyber Solutions
Aon
jason.j.hogg@aon.com

**Christian E. Hoffman**
President—U.S. Cyber Solutions Retail
Aon
christian.hoffman@aon.com
+1.212.441.2263

**Eric Friedberg**
Co-President—Cyber Solutions
Aon
eric.friedberg@aon.com
+1 212.981.6536

**Edward Stroz**
Co-President—Cyber Solutions
Aon
edward.stroz2@aon.com
+1 212.981.6541

**James M. Aquilina**
President, Aon Cyber Solutions
Aon
jaquilina@strozfriedberg.com
+1 310 623 3301

**Thomas E. Abel**
Senior Vice President, Marketing and Business Development—Cyber Solutions
Aon
thomas.abel@aon.com
+1 212 903 2818

**Stephanie Snyder**
Commercial Strategy Leader, Cyber Solutions
Aon
stephanie.snyder@aon.com
+1 312.381.5078
About Aon
Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

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 field of cybersecurity, with leading experts in digital forensics, incident response, proactive security, investigations, intellectual property, and eDiscovery, 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/.

© Aon plc 2018. All rights reserved.
The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

www.aon.com | www.strozfriedberg.com