Cybersecurity risks, challenges and the path forward in wealth and asset management

By Reto Aeberhardt, Jaime Kahan and Richard Wells
September 2016
Cybersecurity continues to be “top of mind” for wealth and asset managers as the number of high-profile attacks continues to increase. The dynamic nature of the sector provides a unique set of challenges in the management of cyber risks. Over the past few years, we have observed firms establishing their strategic priorities and enhancing their adaptability to an interconnected global economy. This includes expanding business in high-growth markets as well as leveraging enterprise intelligence and data analytics as competitive advantages, all of which exposes wealth and asset management to new cyber risks compounded by an ever-evolving threat and regulatory landscape.

It has been estimated that up to 35 million attacks occur for large organizations every year. Typically it takes an organization 200 days to detect an attack. Firms also continue to struggle to keep pace with the threat vectors, with limited resources and budgets.

Cyber risks should not be viewed only as a technology issue, but as a pervasive business and operational risk with the potential for a significant negative impact on assets, revenues, reputation and profitability. An organization’s cyber program should be focused on holistically managing cyber risk and protecting people, processes and technology, as well as protecting investor and other stakeholder value. Managers need to think through the full range of cyber exposures and examine all contributing sources of cyber risk when designing this integral component of the organization’s enterprise risk management process. Regulators around the world are clearly increasing scrutiny on cybersecurity risk management.

Cybersecurity needs to be embedded within a firm’s culture and organization. Managers need to keep a few salient points in mind including that:

- It is not possible to prevent all attacks or breaches.
- The changing business environment will drive newer regulations.
- What companies used to know and do to protect their most valued information is no longer enough.
- Attacks from adversaries outpace traditional cybersecurity security responses.
- Technology-enabled transformation will change the existing cyber risk landscape.
- Early detection of cyber attack will be key.
Facts and trends: operating in a digital world invites new challenges and threats

Cybersecurity threats continue to evolve as attackers become more sophisticated, patient and persistent. Due to the relative ease of access via IP-addresses, digital systems are often targets for cyber criminals and should be included in an organization’s approach to improving cyber maturity. Attack surfaces also continue to expand beyond technology targets; increasingly, the human element is exploited by attackers to gain access to sensitive business data.

Typical points of weakness include:

- Smart devices and services can deliver unintended consequences and mass vulnerable data.
- Social media is 'always on' and information widely shared, without a full appreciation of privacy and security.
- Information is increasingly stored in the cloud or with third parties, resulting in less control, increased risk and a more complex cybersecurity ecosystem.
- Human behaviors are changing.
- New legislation and regulations are forcing changes in processes which can open up new vulnerabilities and widen the attack surface of the organization.
- Reliance on third party outsource and cloud services providers creates additional pathways into an organization.

EY conducts an annual Global Information Security Survey to identify industry trends in security program maturity, security investment prioritization, and preparedness against attacks and data breaches. In 2015, 1,755 respondents representing all key sectors in 67 countries participated in the survey.

According to survey results, respondents from the asset management sector do not feel prepared in their ability to detect attacks and meet increasing cybersecurity demands. Key statistics revealed through our survey included that, in the asset management sector:

- 25% of respondents listed “end user awareness” as the primary control failure that led to the most significant cyber events of the previous year.
- 33% of respondents feel their organization is unlikely to detect a sophisticated attack.
- 60% of respondents say lack of skilled resources is a key challenge for managing IT security.
- 47% of respondents do not have a Security Operations Center (SOC) that is responsible for the identification and resolution of security events.
- 49% of respondents do not have a threat intelligence program.
- 22% of respondents realized a financial impact between $100,000 and $1,000,000 due to information security events over the previous year.
- 51% of respondents spend less than $1,000,000 on information security.
- > 60% of respondents will either invest 5%-15% more on cybersecurity or invest the same as last year.
Increased regulatory requirements – overview

Conventionally, wealth and asset managers have invested heavily in remediating operational risks that maximize returns. As the number of security incidents and attacks intensify, managers need to adopt a proactive approach and familiarize themselves with the relevant regulations. Firms need to reassess their operating models and cybersecurity eco-system and evaluate whether new policies, standards and procedures need to be implemented to strengthen the security controls and overall governance structure and comply with relevant global regulations.

In view of the recent developments in regulatory landscape, the traditional approach of confining regulatory challenges to a compliance officer needs to change. An environment where cybersecurity controls and leading practices are operationalized throughout the organizational structure should be encouraged.

The government mandates and regulatory rules may also increase to combat cyber threat actors in the rapidly evolving digital world which will add to the burden of organizational security management. Organizations need to be aware of the various cybersecurity regulatory requirements as guidance, as well as the differences in requirements amongst the various countries they have a presence in. Continued oversight by the senior management and proactive measures taken across the organizational structure to adhere with the regulatory standards and security controls will help reduce this burden and maintain stakeholder confidence. In addition, organizations must maintain documentation that demonstrates their compliance with their countries' applicable cybersecurity regulations.
Ransomware is the term applied to a broad category of malware that prevents the victim from accessing critical data and functions of a system until a ransom, typically via the digital currency Bitcoin, is paid to the attackers.

It is malicious software, that when executed, encrypts all files on a target system, this can be a local hard disk drive or a server, preventing an authorized user from being able to access them. Attackers hold the files hostage until a ransom is paid. McAfee Labs has seen a 165% rise in ransomware in Q1, especially with the family CTB-Locker, along with new versions of CryptoWall, TorrentLocker, and spikes of BandarChor. Any organization that has high value data is a potential target, which makes the wealth and asset management sector an appealing target in the eyes of malicious actors.

Ransomware can enter an environment through the same channels as other traditional malware – via an infected email attachment, malicious website URL or newsgroup postings etc. The most advanced versions of this malware can spread across the network increasing the number of impacted systems significantly.

Ransomware attacks are occurring more frequently and a new ransomware family has emerged - CTB-Locker. In recent months, headlines have been made as school districts and healthcare organizations were forced to practice crisis management while triaging ransomware attacks.

**Ransomware mitigation strategies include:**

- A security-minded workforce is the best prevention mechanism to any malware attack. Annual security awareness training is no longer enough to mitigate this risk. Introducing email and telephonic phishing tests can test employee readiness to identify and report suspicious behavior.
- A mature system backup and restore process will allow data to be recovered in the case of a ransomware attack by restoring data from a point prior to infection.
- The use of an SOC provides active defense by monitoring, identifying, investigating and resolving security events.
A realistic cyber attack simulation can help you to understand your readiness to respond to a cyber attack — preparing for the inevitable

A response plan that has not been tested is as useful as having no plan. The midst of a security breach is not a good time to test the plan. Regular testing of your cyber incident response plan will help ensure everyone involved is familiar with the business decision making process and ready to react when a critical incident occurs.

For example the Hedge Fund Standards Board (HFSB), the standard-setting body for the hedge fund industry, has held its first tabletop cyber attack simulation in December 2015 for hedge fund managers in London. The goal of the cyber attack simulation was to explore the responses to realistic attack scenarios, including data theft, financial infrastructure attack and crypto ransomware.

The key insights on cybersecurity arising from the simulation were:

- Confusion over responsibilities can prevent an effective response. Managers should not consider cybersecurity as just an “IT” issue, given the legal, compliance, investor relations and reputational issues involved.
- Certain types of cyber attacks may exceed a manager’s internal response capabilities. Managers should be prepared to quickly access external legal and IT expertise.
- Preparation in advance, through a cybersecurity incident response plan, is important. This planning establishes responsibilities, pre-identifies external resources and speeds decisions should there be an actual incident.

Cyber incident response — key challenges

- Keeping your response team current and well-versed in incident response, in the face of competing priorities
- Obtaining executive buy-in and participation in incident response planning and exercises
- Shortage of skills and internal capability to respond to an increasing number of complex attacks
- Learning of a cybersecurity breach from outside sources, such as law enforcement, a regulator or a client.
- Managing the media, when the news of a security breach has already gone viral
- Assuring customers, regulators, investors and other interested parties that the breach is under control

Today’s reality:

- It’s not a crime to be attacked; you can’t stop being a target.
- The real problem is not realizing you’ve been breached, and failing to react in a planned and coordinated manner.

Organizations typically overlook the importance of rehearsing the time-pressured business decision-making that is a critical component of responding to a cybersecurity incident.

Those who fail to prepare will struggle to contain an attack and will feel the impact to a far greater extent. Having a cybersecurity incident response process which manages an incident from identification through investigation, containment, remediation and follow-up is the first step.
Cybersecurity risk, challenges and the path forward

By Reto Aeberhardt, Jaime Kahan and Richard Wells
The scenario outlined below provides an example of a cyber incident simulation that could cause catastrophic impact.

Employees and IT teams arrive into work and can't login to their computers (all logins disabled) across three countries (China, Singapore, United States).

CEO receives email from anonymous attacker attaching executive remuneration information, threatening to disable more business units, and release sensitive, internal and customer data if a ransom demand is not met.

Financial Times reporter receives an email appearing to be from the CEO's account, which informs him of the loss of control of internal systems and the apparent wide scale data theft. Reporter calls the CEO to confirm.

A further 1,500 records relating to US and SG customers are released and employees in HK cannot access computer systems.

CEO receives another ransom email demanding payment of US$100m or all customer data globally will be released along with email data from all top executives.

Businesses in China, Singapore, and United States deal with customer queries.

CEO receives another ransom email demanding payment of US$100m or all customer data globally will be released along with email data from all top executives.

Law firm representing a small group of customers on a contingency basis threatens legal action to claim damages for data loss and fraud monitoring services.

Sensitive customer data for 1,000 CH customers published on file-sharing website.

Customer service centers in the CH and SG are inaccessible and customers start to report issues via social media.

Due to inability to contact via telephone, CH data protection regulator turns up at CH offices looking to speak to "whomever is in charge".

Financial regulator in SG sends enforcement team to investigate.

SG police investigators arrive at SG offices on foot of media reports surrounding extortion attempts.

Widespread speculation on social media and multiple media requests for comment and statement in various countries. Regulators in multiple jurisdictions are demanding updates and irregularities in the trading systems reported.
Ten point action plan: The following are 10 considerations that managers should include when creating and updating their organization’s cybersecurity program:

1. Understand the business ecosystem including understanding internal and external stakeholders that impact business strategy and operations, threat actors across the ecosystem and understand how cybersecurity impacts your strategy and business relationships.

2. Identify your most critical assets (crown jewels), threat scenarios and the potential impact to your bottom line if compromised.

3. Prepare and assist your board and organization to mitigate operational, economic and reputational risks in response to a breach.

4. Define your cyber risk appetite and develop a cybersecurity strategy to help achieve your vision while maintaining agility and resilience.

5. Improve cybersecurity awareness and focus on creating a security-minded workforce.

6. Embed cybersecurity into your operating model, business architecture and operations through digital and cybersecurity transformation.

7. Extend your cybersecurity framework with more detection mechanism and extend your SOC capabilities and incorporate cyber threat intelligence.

8. Test your cyber incident response plan.

9. Optimize your resilience strategy.

10. Evaluate cyber insurance packages to properly cover you in the event of a breach.
Attackers have access to significant funding; they are more patient and sophisticated than ever before; and they are looking for vulnerabilities in the whole operating environment — including people and processes.

The resilience of digital systems becomes more and more important and more and more challenging at the same time. New technologies, regulatory pressure and changing business requirements call for more cybersecurity. However, securing digital systems is not an easy task due to the complexities of the digital environments, legacy systems, and different vendor architectures.

So what can firms do to help manage cybersecurity threats? This question is an especially challenging one, as new threat vectors emerge every day, often in unexpected areas. Executives need a cybersecurity lens on all aspects of the business: strategy, finance, operations, regulatory. Digital touches every part of your business, so cybersecurity needs to as well. Firms should work to develop a prudent cybersecurity risk management framework that can adapt to any threat that emerges. Organizations must remain diligent in supporting their firm's cybersecurity program and continue to adapt to changing environment and especially including more attack detection mechanism in within their environment.

If you don't know you've been hacked, how do you assure your investors they're protected?

Summary
# Contacts

<table>
<thead>
<tr>
<th>Country</th>
<th>Person of contact</th>
<th>E-Mail</th>
<th>Phone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>Nuvin Goonmeter</td>
<td><a href="mailto:nuvin.goonmeter@fr.ey.com">nuvin.goonmeter@fr.ey.com</a></td>
<td>+33 1 46 93 64 55</td>
</tr>
<tr>
<td>Germany</td>
<td>Lars Weimer</td>
<td><a href="mailto:lars.weimer@de.ey.com">lars.weimer@de.ey.com</a></td>
<td>+49 619 6996 27489</td>
</tr>
<tr>
<td>Ireland</td>
<td>Hugh Callaghan</td>
<td><a href="mailto:hugh.callaghan@ie.ey.com">hugh.callaghan@ie.ey.com</a></td>
<td>+353 1 2212 411</td>
</tr>
<tr>
<td>Italy</td>
<td>Marco Calzolaio</td>
<td><a href="mailto:marco.calzolaio@it.ey.com">marco.calzolaio@it.ey.com</a></td>
<td>+39 02 8066 92277</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>François Barret</td>
<td><a href="mailto:francois.barret@lu.ey.com">francois.barret@lu.ey.com</a></td>
<td>+35 24 212 48547</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Stijn Giesberts</td>
<td><a href="mailto:stijn.giesberts@nl.ey.com">stijn.giesberts@nl.ey.com</a></td>
<td>+31 88 407 13 20</td>
</tr>
<tr>
<td>Switzerland</td>
<td>Reto Aeberhardt</td>
<td><a href="mailto:reto.aeberhardt@ch.ey.com">reto.aeberhardt@ch.ey.com</a></td>
<td>+41 58 286 67 40</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>Rebecca Cox</td>
<td><a href="mailto:rcox@uk.ey.com">rcox@uk.ey.com</a></td>
<td>+44 20 7951 3671</td>
</tr>
</tbody>
</table>
About the global EY organization
The global EY organization is a leader in assurance, tax, transaction and advisory services. We leverage our experience, knowledge and services to help build trust and confidence in the capital markets and in economies all over the world. We are ideally equipped for this task – with well trained employees, strong teams, excellent services and outstanding client relations. Our global purpose is to drive progress and make a difference by building a better working world – for our people, for our clients and for our communities.

The global EY organization refers to all member firms of Ernst & Young Global Limited (EYG). Each EYG member firm is a separate legal entity and has no liability for another such entity’s acts or omissions. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information, please visit www.ey.com.

EY’s organization is represented in Switzerland by Ernst & Young Ltd, Basel, with 10 offices across Switzerland, and in Liechtenstein by Ernst & Young AG, Vaduz. In this publication, “EY” and “we” refer to Ernst & Young Ltd, Basel, a member firm of Ernst & Young Global Limited.

© 2016
Ernst & Young Ltd
All Rights Reserved.
ED None

This publication contains information in summary form and is therefore intended for general guidance only. Although prepared with utmost care this publication is not intended to be a substitute for detailed research or professional advice. Therefore, by reading this publication, you agree that no liability for correctness, completeness and/or currentness will be assumed. It is solely the responsibility of the readers to decide whether and in what form the information made available is relevant for their purposes. Neither Ernst & Young Ltd nor any other member of the global EY organization accepts any responsibility. On any specific matter, reference should be made to the appropriate advisor.

www.ey.com/ch