accenture consulting

InsideOps | Insights for Operations Leaders

Cybersecurity for Asset Managers: Shielding Your Firm from Risks

High performance. Delivered.

Strategy | Consulting | Digital | Technology | Operations

Data breaches. Ransomware. Spoofing. Phishing. Identity theft. Bot attacks. Wire fraud.

These terms have become part of our vocabulary. Make that part of our daily vernacular. There's a reason for that. These types of cybercrimes are rampant—and the financial services sector is a prime target. That's what cyber experts, regulatory bodies and many in the financial services community, including asset managers, told us in Accenture's High Performance Security Report 2016. A cross-section of 275 leaders in the financial services industry participated in the survey, which uncovered:

85 data breaches per year

Average number of targeted security breaches that a typical financial services firm faces.

33% will succeed

Share of attacks that result in a problem or destruction—that's 2 to 3 per month.

68% are unknown

Share of firms that consider cyberattacks a "bit of a black box."

48% come from inside

Share of respondents who say the greatest security risk arises from internal sources.

59% take months to detect

Share of firms that think the bad guys have plenty of time to achieve their objectives.

14% aren't discovered for a year or more

Share of firms that discover effective attacks long after they probably occurred.

Source: Accenture High Performance Security Report 2016

In light of the frequency and complexity of cyber risks, asset managers should operate on the assumption that breaches will occur. It's unlikely that firms can prevent cyber menaces from infiltrating barriers all of the time. Attacks will crop up.

What's an asset manager to do? Develop a robust cybersecurity program that's designed to prevent attackers from achieving their objectives, rather than simply prevent breaches. Like cybercrimes themselves, cybersecurity initiatives need to be multifaceted. Above all, firms need to "think resilient."

Building cyber resiliency

Cyber resiliency is the ability to operate business processes in normal and difficult scenarios without adverse outcomes. Resiliency strengthens a firm's ability to identify, thwart, detect and respond to process or technology failures. It also bolsters a firm's ability to quickly return to business as usual if an attack occurs, while reducing financial loss, customer harm and reputational damage.

Businesses with cyber resiliencies in place have several characteristics in common:

- Secure processes and systems
- Strong controls with a strong control environment
- Digitized and automated processes
- An aggressive, proactive and enterprise-wide culture that prioritizes security

Cyber resiliency helps a firm to detect, respond to, identify, prevent and recover from an attack.

To become more cyber resilient, firms should not only incorporate perimeter security, but also implement business risk/reward decision making, cyber risk management and control techniques throughout their business processes. They should also secure buy-in from the organization's leadership.

Creating cyber resiliency, however, spans business processes and infrastructure. For example, it should include re-architecting business processes to reduce access to, dissemination of and reliance on highly sensitive data. It should also involve recasting infrastructure and systems to limit damage when an attack occurs or systems and processes fail. And it may include reworking how legal and liability protections are incorporated into service agreements to prevent fraud-related losses or expenses associated with remediating impacted customers.

Protecting the "secret sauce"

Asset managers work hard to develop strategies, and accumulate and organize information, for their firms—efforts they don't want to put at risk. Those in the industry refer to the items in this valued repository as the "secret sauce." Without cyber resilience and proper solutions in place, asset managers will be hard-pressed to protect the following prized assets of their own from security breaches:

Segment	Vulnerability
Front office	Systems and data, including: • Proprietary algorithms • Models • Analytics • Trades • Trade routing and execution patterns • Proprietary research
Middle office	Systems and data related to: • Positions • Trade files • Performance analytics • Institutional and private client accounts
Back office	Internal and external repositories for: • Trade files • Positions • Retail investor data at transfer agencies
Sales and distribution	Confidential information on: • Sales prospects • New clients • Growth strategies
General	Internal communications on: • Acquisition strategies • Earnings releases • Routine business matters that could affect reputation

Laying the foundation for cybersecurity

What should an asset management firm do to try to safeguard the secret sauce and achieve cyber resiliency in principle and practice?

1. Think, act and live cybersecurity.

Cyber criminals' avenues of access can be everywhere, so all hands, eyes and ears need to be attuned to the possibilities. Embracing enterprise-wide cybersecurity is a mindset that involves changing behaviors and making security a cornerstone of the firm's culture. Cybersecurity is more than anti-virus software—it's educating and empowering employees to make smarter decisions, and supporting them with proper processes and technologies.

2. Ask stakeholders to be on the lookout.

Engage all stakeholders, including suppliers, partners and even clients. Develop third-party cybersecurity clauses, provisions and testing in outsourcing due diligence reviews and in service line agreements. Confirm vendors have the necessary ammunition and back-up to detect, respond to and sustain operations in the event of an attack. Explain the security program to partners and clients and ask them to report anything unusual.

Cybersecurity is no longer the responsibility of IT alone. Today, all stakeholders associated with firms have roles to play.

3. Take a holistic approach when building your defense.

Cybersecurity is no longer the responsibility of IT alone. It requires involvement from across the organization and multiple lines of defense. Businesses should assess cybersecurity incident scenarios to better understand those that could materially affect the firm. Bringing business executives and IT to the table together can help to promote cybersecurity as a strategic imperative and integrate it into the firm's highest-level plans.

4. Go extreme: double down and tech up.

Vigilance and allied focus on security are vital. So are the right perspectives and tools to address the problems. Rethink policies, processes and permissions; reassess procedures in light of the plight to protect and extend your firm's value. Perform application reviews; classify, embed and encrypt. Use melded approaches to help your organization to avert, identify and promptly recover from attacks and outages caused by both internal and external sources.

Get the best solutions—whether they're inside the firm, beyond the firm or both. That may involve:

- Real-time network monitoring using intelligent automation to spot and block suspicious activity.
- Secure virtual environments and processes.
- Outside hosting of trading or settlement applications.
- Improved identity and access management technology.
- Heightened visibility and control over individual user access.
- Cloud computing technologies with enhanced controls and protections.

5. Put your cybersecurity to the test.

Keep your cyber security initiative front and center with periodic training and communications. Like the world of cybercrime, the quest for security must be constantly evolving.

Accenture recommends a two-pronged approach focused on cybersecurity assessment and attack simulation. Each of these activities on its own can provide valuable insights into an organization's security program. When they're combined and performed periodically in parallel, it becomes easier to see where and how to focus critical resources.

In this testing domain, Accenture puts its own spin on the two-pronged approach. It starts with a risk assessment that emulates what cyber criminals do, using their favorite tools, tactics and techniques. This method reveals a client's main vulnerabilities from the mindset of those interested in puncturing the safeguards the firm has put in place. Based on the findings of the assessment, a simulation is developed. Experience shows that this step is eye-opening.

Four factors to keep in mind

1. Governance and leadership

Develop a cybersecurity chain of command to lead the initiative and nurture a security-minded culture. With access to firm executives and the enterprise as a whole, a cybersecurity team can establish the pillars of the program. Members can set parameters for accountability, establish policies and programs, create incentives, and provide cybersecurity performance and updates.

2. Regulatory requirements

Several years ago, the United States Securities and Exchange Commission (SEC) alerted the financial community about an increasing spate of cyberattacks on the sector. It now requires firms to adopt written policies to protect clients' private information, anticipate potential cybersecurity events, and have clear procedures in place instead of reacting to a breach after it occurs. Guidance documents recommend additional measures that funds and advisors may wish to consider when developing cybersecurity resiliency.[1]

3. Risk tolerance

Cyber criminals always are looking for new ways to infiltrate barriers. It's their job. Similarly, those leading the cybersecurity charge—and everyone for that matter—need to be as dedicated to building defenses as those who seek to topple them. When developing their cybersecurity initiatives, firms need to weigh the potential threats against their appetite for risk by gathering information, questioning and simulating the types of attacks they're most likely to face.

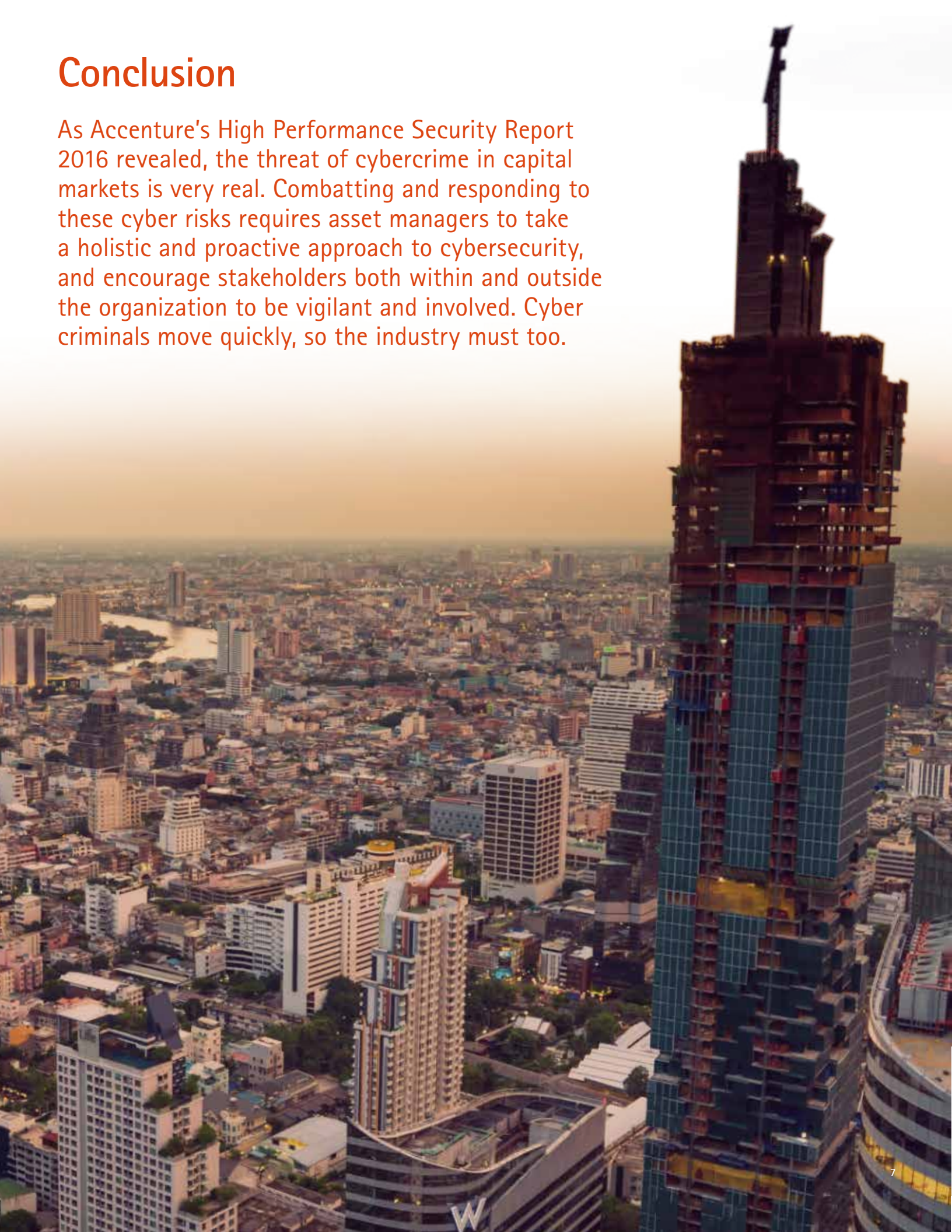
4. Return on investment

Forging an initiative to instill resilient cybersecurity comes at a cost—but not having a robust program does too. In the latter case, costs may take the form of data losses, interruptions to operations, regulatory consequences, lost clients and reputational damage. When determining how much to invest in cybersecurity, firms need to consider the potential return on investment (ROI).

It's imperative for asset managers to adopt proper policies and procedures. Pronto.

Conclusion

As Accenture's High Performance Security Report 2016 revealed, the threat of cybercrime in capital markets is very real. Combatting and responding to these cyber risks requires asset managers to take a holistic and proactive approach to cybersecurity, and encourage stakeholders both within and outside the organization to be vigilant and involved. Cyber criminals move quickly, so the industry must too.



Contacts

Girard Healy
Managing Director
girard.healy@accenture.com

Chris E. Thompson
Accenture Financial Services
Finance & Risk Lead
chris.e.thompson@accenture.com

Follow us on Twitter
@AccentureCapMkt

Follow us on LinkedIn
https://www.linkedin.com/showcase/10561616/

Explore more Latest Thinking
www.accenture.com/AssetManagement

Reference

1 https://www.sec.gov/investment/im-guidance-2015-02.pdf.

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions – underpinned by the world's largest delivery network – Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 401,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

172025