Deloitte.

Transforming cybersecurity:
New approaches for an evolving threat landscape

By the numbers: Current threat environment for financial services firms

#1

The financial services industry topped the list of 26 different industries that cyber criminals most targeted[1]

$23.6 million

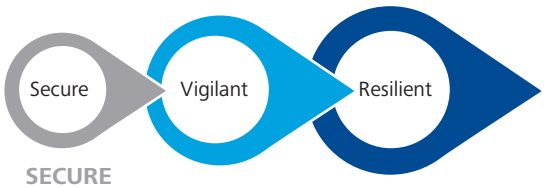
Amount lost from cybersecurity breaches last year[2]

88% of cyber attacks are successful in less than one day. But in the same time period, only **21%** of firms are able to discover attacks, and just **40%** are able to restore their business[3]

36% of financial services institutions are most concerned about financial losses resulting from cyber attacks. But what may be more concerning, as indicated by **39%** of firms, are disruptions to the business and reputational risks[4]

37% of financial services companies believe individual hackers pose the greatest danger to their organization, and **29%** believe insiders and third parties may be the biggest threats[5]

Where can firms go from here? Creating a "secure, vigilant, and resilient" strategy



SECURE
Enhance risk prioritized controls to protect against known and emerging threats and comply with industry cybersecurity standards and regulations

VIGILANT
Detect violations and anomalies through better situational awareness across the environment

RESILIENT
Establish the ability to quickly return to normal operations and repair damage to the business

Getting there: Two important levers financial services firms can implement to manage evolving cyber threats

Actionable threat intelligence

- Experience-based learning
- Situational awareness

Strategic organizational approach

- Executive sponsorship
- Dedicated threat-management team
- Focus on automation and analytics
- People and culture
- External collaboration

Take five: Potential actions leaders can take to implement a comprehensive, organizational approach to cybersecurity

1
Cyber risk strategy to be driven at the executive level as an integral part of the core company strategy

2
A dedicated cyber threat management team to be established for a dynamic, intelligence-driven approach to security

3
A focused effort to be placed on automation and analytics to create internal and external risk transparency

4
The "people" link in the defense chain can be strengthened as part of a cyber risk-aware culture

5
Cybersecurity collaboration to be extended beyond company walls to address common enemies

Contact

To learn more about the Deloitte Center for Financial Services, its solutions, thought leadership, and events please visit:

www.deloitte.com/us/cfs

Subscribe

To receive email communications, please register at:

www.deloitte.com/us/cfs

Engage

Follow us on Twitter at:

@DeloitteFinSvcs

For more information and to download the full report, please visit www.deloitte.com/us/cfs/cybersecurity.

Deloitte Center
for Financial Services

The Deloitte Center for Financial Services offers actionable insights to assist senior-level executives in the industry to make impactful business decisions.

[1] "Not Your Average Cybercriminal: A Look at the Diverse Threats to the Financial Services Industry," Mandiant, September 23, 2013.
[2] "2013 Cost of Cyber Crime Study: United States," Ponemon Institute (sponsored by HP Enterprise Security), October 2013.
[3] Verizon Risk and Deloitte Center for Financial Services analysis.
[4] Deloitte Dbriefs, Cybersecurity—Evolving approaches in a more complex world, December 10, 2013.
[5] Ibid.