EXECUTIVE BRIEF

CYBER ATTACKS ON THE FINANCIAL SECTOR - ASSESSING RISKS

- Insights for busy professionals
- Read in less than 10 mins
- Knowledge without the fluff

Underwritten by:

insight brief
RESEARCH. DISCOVERY. INSIGHTS.

esentire®

RFG

THIS EXECUTIVE BRIEF IS A SUMMARY OF THE WHITE PAPER:

The "Inevitable" Cyber Attack: Are You Prepared?

CLICK TO ACCESS THE FULL WHITE PAPER

INTRODUCTION

- Cyber-attacks are a fact of life. They are increasing in volume, becoming more sophisticated and are more frequently targeting the financial sector and its service providers.

KEY POINTS

- Cyber-criminals consider smaller and mid-size financial organizations such as hedge funds, private equity funds and registered investment advisers particularly easy targets.
- Hedge funds and other financial service businesses have been targeted by hackers with sophisticated, credible emails with often undetectable Trojan bearing attachments installing key loggers that upload financial data to the hackers' servers.
- Smaller and mid-size financial organizations are attractive to cyber-criminals because they have confidential data on clients, data on corporate investment strategies and models and sensitive material on mergers.
- Cyber-attacks may be politically motivated as they harvest sensitive data that can be used to influence decision making.
- The risk of theft of sensitive information and intellectual property from an organization is largely unregulated by financial regulators.
- Smaller and mid-size financial organizations provide cyber-criminals with a conduit to other targets including service providers (banks and brokerages) and law firms.
- Cyber-attacks also can be acts of terrorism. Vulnerability to this threat is compounded by the interconnectivity of the system.
- Activist hackers have a record of attempting to destroy a business's reputation by defacing websites and leaking data.
- Cyber-criminals access target networks through email with spyware attachments (phishing). These emails often contain specific information relevant to the target business that seems to come from a reliable source (spear-phishing).

KEY POINTS (cont.)

- Generally most defenses against hacking are not effective. Security breaches often go undiscovered for months and most are discovered by external parties, not the targeted company itself.
- The SEC, recognizing the escalation of cyber-attacks, is quickly adopting appropriate steps to deal with cyber-crime.
- The real threat of cyber-terrorism leads to expanding regulatory activity that affects every organization as it prepares for the "inevitable" attack.
- The framework for security established by the NIST will combine legal and regulatory security requirements and best practices.

IMPORTANT FINDINGS

- Data collected by eSentire indicates a 100% increase in targeted attacks over the previous year.
- Cyber-security is frequently easier to breach in smaller financial organizations than in larger ones.
- The trend in cyber-crime indicates that most companies will be hacked and many will be hacked again.
- Hackers increasingly infiltrate networks installing "drive-by-downloads" adding malicious material to websites. eSentire reported a 10% increase in "drive-by-downloads" in 2013.
- New criminal initiatives include attempts to extort payment for hacked data, compromising operational uptime, reducing profits and performance. Business disruption and loss of reputation may be spread to trading partners.
- Hackers' malicious scans for defense vulnerabilities increased by 20% in 2013 according to eSentire.
- Hackers are not only often successful in stealing funds from small to mid-size businesses and law firm trust accounts but they also target firms involved in significant financial transactions to acquire sensitive information.
- "Advanced" cyber-threats or "sleepers" work on an organization's network in three phases. Hackers first establish beachheads inside a business by creating new viruses or outflanking defenses.
- In the second phase, "sleepers" acquire control of security systems and disarm anti-virus software.
- In the third stage a "sleeper" allows hackers to access confidential information and, in a more recent twist, to encrypt a company's data for which hackers demand a ransom before providing the encryption key.

IMPORTANT FINDINGS (cont.)

- Hackers may gain access to systems through trusted advisors. Law firms are a common mark as they provide access to their clients' networks.
- Risk assessments by eSentire have revealed that every company studied had high or critical security vulnerabilities.
- Mobile devices with remote access to business networks are particularly vulnerable to web-based attacks.
- A new attack detected by eSentire used Microsoft Word files to carry malware.
- Anti-virus vendors are often slow to recognize new threats. A single breach can spread instantly throughout a network.
- Regulatory agencies are concerned with the security of personal information to protect against financial loss but cyber-criminals have developed new initiatives that go beyond this motive.

TAKEAWAYS

- Meeting current regulatory standards is insufficient for small and medium sized financial businesses. Improving critical infrastructure for cybersecurity is a new mandate of the National Institute of Standards and Technology which will create non-prescriptive guidelines.
- To prepare for the inevitable cyber-attack a financial services business must do a risk assessment of their firm. This should be accompanied by an enterprise-wide vulnerability assessment and an assessment of the security of IT service providers and ancillary information sharing systems.
- Risk assessment analysis for firms involved in financial services should include a list of regulators of the firm and regulators overseeing clients and investors
- Security of sensitive personal information is regulated by financial and legislative initiatives. Best practices for business cyber-security include the creation of a security and privacy policy, designation of an employee to oversee the security program and internal and external testing of security measures.

CLICK TO ACCESS THE FULL WHITE PAPER

Share this document

Click or scan t o access the full white paper

Click to access the full white paper

Share this document

eSentire® is the leader in Active Threat Protection solutions and services, the most comprehensive way to defend enterprises from advanced and never-before-seen cyber threats. eSentire's flagship offering, Network Interceptor, challenges legacy security approaches, combining behavior-based analytics, immediate mitigation and actionable intelligence on a 24x7x365 basis. The company's dedicated team of security experts continuously monitors customer networks to detect and block cyber attacks in real-time. Protecting more than $2.0 trillion in combined assets, eSentire is the trusted choice for security decision-makers in financial services, healthcare, mining, energy, engineering and construction, legal services, and technology companies.

"Since its founding in 2009, RFG has helped clients proactively address the increasingly complex regulatory and legal requirements they face when engaging in investment activities. Today RFG represents clients which have more than $100 billion in assets under management, including a consortium of the nation's leading endowment investment offices.

ABOUT INSIGHTBRIEF

Our team produces short documents for busy professionals, summarising longer reports and research papers so that readers can swiftly become acquainted with a large body of knowledge and decide whether or not to read the full source document(s).

We vet and qualify reports for relevancy and value to its intended audience before creating an InsightBrief document. Our editorial team is independent from the originator of the report, ensuring that the insights exclude sales or vendor centric messaging, thereby creating real value for our time-poor readers.