Financial Services Cyber Security Guide

The Financial Services Cyber Challenge

Our world has been radically transformed by digital technology – smart phones, tablets, and web-enabled devices have altered our daily lives, including the way we do commerce and manage our finances. At the same time, technology has enabled a new generation of criminals to gain access to corporate and personal sensitive data.

Verizon's *2016 Data Breach Incident report* (DBIR) revealed that web application attacks and unauthorized data transfer continue to be most widespread types of data loss. Phishing through malicious email, installing crime-ware, and exploiting weak or stolen credentials are the most effective ways criminals gain access to information assets. In fact, 30% of phishing messages were opened by the target across all campaigns, a significant increase from 2015.

PricewaterhouseCoopers' (PwC) 2014 Global State of Information Security Survey revealed that 45% of Financial Services organizations have suffered economic crime as opposed to 34% of all other sectors in 2014. Cyber crime is on the rise, and defenses are falling behind. The survey paints an eye-opening picture: "While many have made significant security improvements, most companies are still falling behind today's determined adversaries."

The Solution

With greater usage of cloud-based applications, the Internet of Things, and increased data privacy requirements, financial services are taking the steps needed to protect the confidentiality, integrity, and availability of sensitive data and to comply with FINRA and other industry compliances.

The four key components of a solid internet and data security program include:

- Advanced Threat Defense
- Education of Staff and Vendors
- Data Protection Services
- Endpoint Security

Advanced Threat Defense

Email is a primary threat vector by which hackers access your client data. It's easier for a hacker to send out an email than to hack a firewall – it takes just one unsuspecting staff member to open the wrong email or click a bad link to punch a hole in your network defense. EdgeWave's ePrism Email Security Suite includes the powerful tools you need to assure the protection of private data, and the efficient delivery of legitimate email. ePrism offers fully hosted in-the-cloud services that require minimal management, are affordable, and can scale easily to fit any size network.

ePrism includes a multi-layered approach that stops emerging threats before they can get near your network. EdgeWave cybersecurity solutions combines human threat review and automated intelligence to identify and stop advanced threats in real time. Humans can identify the intent of inbound threats in a way an algorithm can't – that's why every cyber security plan must include human analysis. In 2016 alone, our human review process has blocked over 120 million malicious emails per day with human-written rules and analysis. The 2016 Verizon Data Breach report promised "We may be able to reduce the majority of attacks by focusing on a handful of attack patterns." EdgeWave's EPIC leads the market with this capability.

Data Protection Services

Data Loss Protection (DLP) - ePrism includes a content analysis and policy engine that uses proprietary technology to detect private information transmitted via outgoing email. This data protection technology analyzes data in motion, and using compliance-based rules, detects and blocks any sensitive private data trying to leave your network. This solution is easily managed from the ePrism Central Dashboard giving you the powerful tools you need to comply with FINRA and other regulatory guidelines.

Encryption - EdgeWave Email Encryption assures the secure delivery of email to anyone outside your network, with next-generation technology that eliminates the cost and complexity associated with many traditional encryption services. As a completely hosted service, there is no hardware or software to implement. Encryption can be easily enabled on a per user basis or as part of an automated routing policy. In addition, because it is integrated into the ePrism Hosted Email Security and Data Loss Protection services, your outgoing email is inspected for malware, viruses, inappropriate content, compliance breaches and violations of your acceptable use policy (AUP). You can manually encrypt messages or configure to automatically encrypt per a variety of factors; such as sender, recipient, or when DLP problems are detected.

Endpoint Security

Mobile devices such as tablets, phones, and laptops have found their way into Financial Services whether you like it or not. Your agents and representatives want flexibility in how they communicate with clients, but this puts regulated personal and financial data at risk.

iPrism Web Security can help you mitigate endpoint risk with Cloud-Based Remote Web Filtering and Mobile Device Security. These security solutions employ proprietary technology to bring powerful Enterprise Web Filtering to all staff and devices, even outside the network. You receive comprehensive protection from web-based threats, granular policy controls, and selective data wiping -- all with centralized administration and reporting. Suitable for both corporate and BYOD devices, iPrism provides anytime, anywhere any device security for iPads, iPhones, Android devices, Windows laptops and Macbooks.

Education of Staff and Vendors

The internet and data security technologies described above are only as effective as the training and policies that enforce their use. Here are 5 steps to get you started on the path to ensuring your organization will support your security efforts:

1. Integrate a security strategy with every plan and initiative. Security is no longer an afterthought in Finance
2. Empower employees with intensive, regular regulatory compliance training. Training must include knowledge of government and industry regulations regarding investor protection
3. Implement and enforce strong organizational/IT policies regarding social media and portable devices.
4. Ensure all employees know how to guard authentication credentials. Require a signed and sealed agreement of understanding and adherence to privacy policies
5. Employ an agile, robust, platform-agnostic, advanced threat detection system that includes encryption

EdgeWave's award winning solutions have helped thousands of financial services organizations protect their data and networks. EdgeWave offers cloud-based services as well as on premise appliances for email and Web security services that require minimal management, are affordable, and can scale easily to fit any size network. To learn more about EdgeWave and its powerful solutions, please visit https://www.edgewave.com/.

4225 Executive Sq, Ste 1600,
La Jolla, CA 92037

Give us a call:
1-800-782-3762

Send us an email:
info@edgewave.com

For more info, visit us at:
www.edgewave.com