DS news

DEFAULT SERVICING » IN PRINT AND ONLINE ... OM » 04.2016

COVER FEATURE PAGE 66

MOVING WITH THE MARKET

WHAT OPPORTUNITIES CAN BE HAD IN SINGLE FAMILY RENTALS?

PAGE 70

STAYING AHEAD OF THE THREAT
WHY SECURITY AWARENESS IS VITAL TO YOUR ORGANIZATION

PAGE 74

DUKING IT OUT
CONGRESS GETS IN THE RING OVER NON-PERFORMING LOAN SALES

12% 12 PERCENT OF THE AMERICAN POPULATION LIVES IN RENTAL HOUSES

15 MILLION THIS 12 PERCENT IS SOMEWHERE IN THE NEIGHBORHOOD OF 15 MILLION HOUSEHOLDS

2 TRILLION $2 TRILLION POTENTIAL MARKETPLACE

INDUSTRY INSIGHT / MICHAEL O'CONNOR

STAYING AHEAD OF THE THREAT

Why Security Awareness is Vital to Your Organization

Data is the lifeblood of banking and financial services organizations. Lenders, appraisers, real estate brokers, and property preservation companies each have the responsibility of protecting and securing financial data. Almost all data generated or used by financial services firms is regulated. The responsibility of managing account information, cardholder data and transactions, and non-public personal information makes this industry, arguably, one of the largest collectors of sensitive and privacy protected data.

The financial services industry continues to invest in new technologies that allow for efficient management of client information with increasing oversight capabilities. However, a concurrent effort to protect information from attack is critical, as evidenced by recent data breaches at high profile organizations including hospital facilities, large retailers, and health care insurers.

In today's world, most organizations, regardless of size, will experience a security incident in the form of social engineering, a data breach, or malware. Social engineering attacks will continue to be the easiest way for cyber criminals to compromise corporate networks. The advanced technology and systems used to protect networks makes the front door approach less appetizing to would be attackers. With social

> "In today's world, most organizations, regardless of size, will experience a security incident in the form of social engineering, a data breach, or malware."

engineering, the attacker can mass engineer an attack with the knowledge that one user can compromise an entire network. Here are a few examples of the types of external security incidents of which organizations should be aware.

- **SPEAR PHISHING:** email spoofing fraud attempt, targeting an organization, seeking unauthorized access to data;
- **WHALE PHISHING/WHALING:** targets C-level users, or users with elevated access to sensitive data;
- **MALWARE/ANTI-VIRUS:** malware is software that disables or damages a computer system;
- **DISTRIBUTED DENIAL OF SERVICE (DDOS):** multiple infected systems are targeted at a corporate network or website causing a denial of service;
- **HACKTIVISM:** the act of compromising a system for socially or politically motivated purposes;
- **EXTORTION HACKS:** cybercriminals threaten to release sensitive data if an organization does not meet some demand;
- **RANSOMWARE:** prevents access to data on a PC by encrypting it and requesting a ransom to unencrypt it.

IDENTIFYING INTERNAL VULNERABILITIES

A data breach occurs when sensitive, confidential, or protected information is obtained by an unauthorized individual or organization. Organizations can improve the security of sensitive data by focusing on controlling how employees access, transmit, and manage documentation. Here are three common areas where, when controlled, organizations can strengthen the protection of sensitive data.

- **SPREADSHEETS:** ensure files are password protected, saved on network drives instead of local hard drives, and access is restricted to authorized users
- **EMAIL AND FILE ATTACHMENTS:** effective email policies, spam filters, scanning email attachments, and encryption improve email security
- **IDENTITY LIFECYCLE:** as users join the organization, move within the organization, and leave the organization their access is always appropriate to their job role and function

Identity is a major attack vector for advanced threats, with compromised credentials being a significant enabler in successful attacks. Organizations need a reliable way to continuously determine that users are who they say they are before allowing access to sensitive data. Attempts to lock down systems and resources with strong authentication too often detract from the user experience, encouraging users to find workarounds that further increase risk. Today's authentication solutions need to be easy to implement wherever authentication is required and allow organizations to optimize the right level of security and convenience for the risks that are present. Organizations with successful authentication strategies will greatly strengthen their security posture while making users' lives easier in the process.

Determining where an organization is vulnerable to the occurrence of a data breach or attack is the first step in protecting sensitive data. However, organizations need to invest in a proactive and flexible strategy that can evolve at the same pace of potential, and inevitable, threats to security.

The financial services industry interacts with a myriad of third-party vendors to perform a variety of business services. Collaborative development, extended supply chains, and outsourced services are just a few ways in which third parties help deliver a competitive advantage. But these third-party interactions create new sources of risk that can significantly impact the organization if not managed proactively. Organizations who work with third parties must develop a systemic process for assessing, tracking, and managing third-party risk. In addition, they must incorporate information regarding risk into their organization's overall risk assessment and management strategy. Organizations that harness this risk are positioned to take advantage of the opportunities afforded by working with third parties to safely drive their business forward.

PROACTIVE SECURITY

The goal of any security program includes proactive protection against attack, a reduction in time to detect a breach, maintaining systems to protect sensitive data, and to have the appropriate procedures and systems in place for business continuity.

The majority of security incidents are caused by human error related to lack of employee awareness and training. Organizations should take a holistic approach to security, however, the first line of defense begins with continual training. Establishing a 'Culture of Security' with your executive management and employees is critical. While investing in IT security is necessary, the best security teams in the world cannot protect against employee failure to recognize targeted attacks. The nature of social engineering means that the cybercriminal has to succeed only once, while your organization has to be successful in protecting against such attacks every time.

Some suggestions to educate your workforce include:

- Communicate regularly using relevant news articles to highlight security as a real threat to business
- Use a variety of mediums to reach your entire audience
- Spread the importance of safe online practices
- Enforce adherence to security policies and procedures at all times

Having security policies and procedures in place will provide your organization with a solid framework when it comes to managing security incidents. The ISO 27001 Information Security Management System (ISMS) provides such a framework for Information Security Management best practices helping organizations to:

- Protect client and employee information
- Manage risk to information security
- Achieve compliance requirements
- Protect the organization's brand image

While ISO27001 will not necessarily prevent a security incident from occurring, it will help ensure that all risks related to security are considered and appropriately managed.

Minimizing the impact of advanced attacks requires a robust capability to detect and respond. Having a formal incident response

plan, and carrying out regular Business Continuity Plan (BCP) exercises, help ensure that organizations are prepared for such events. In an environment of persistent attack, and near-constant compromise, incident response must be a priority for any organization responsible for financial information, personally identifiable information, or intellectual property. Organizational strategies must be based on proven best practices, and they must leverage expertise where required. Security programs must incorporate opportunities to automate and to constantly improve. Organizations with a robust incident response and business continuity capability will have the best chance of minimizing damage or loss from attack.

While social engineering attacks are currently prevalent, threats continue to evolve and take many other forms. Today's workforce is more flexible, cross-functional, and mobile than ever. IT-driven organizations require rapid on-boarding of employees to apps, systems, and resources so that they can be productive right away. Traditional firewall approaches to network security are not enough anymore and organizations must secure data whether it resides inside or outside of the network.

A holistic approach must be taken to consider all points of entry into proprietary systems and all software integrations. The traditional closed network is no longer a reality for today's businesses. The need to connect to clients, vendors, and third-party systems creates a complex network which spans outside of the organization. Protecting these expansive networks requires a multi-disciplined approach to manage organizational risk and meet compliance requirements.

Networks can be compromised without an organization's knowledge. These attacks can be silently mining data without raising any alerts or alarms. It is through regular audits across the network environment that this can be avoided.

Auditing organizational processes and procedures is a not a new requirement for loan servicers, asset managers, appraisers, and property preservation providers, all of whom are all subject to the audit provisions established by the Dodd-Frank Act. Ensuring that regular audits are performed on internal and external systems is as important as the audits required for compliance within the industry. These audits will highlight anomalies on the network, your property platform, and in relation to user access and activity within systems. Audit trails for sensitive data are vital in any system. Knowing how, when, and who last updated a particular sensitive data point can give a degree of comfort when it comes to understanding potential security flaws and preventing them in the future.

Loan servicers, asset managers, appraisers, and property preservation providers require anytime, anywhere access to borrower and asset information. Technology solutions must enforce secure access consistently across internal IT systems, third-party applications, mobile-based apps, and infrastructure. These solutions must balance security and convenience, while ensuring users have access to any information appropriate to their role. Secure access will empower employees and ensure that valuable information remains protected.

TAKING MEASURES FOR PHYSICAL SECURITY

Organizations can minimize their exposure to data breach by taking an inventory of physical opportunities to reduce vulnerabilities. Physical procedures include:

- Locking laptops in cabinets and/or car trunks
- Locking screens when employees leave their workstations
- Providing privacy screens on computer monitors
- Disabling ability to download data onto external drives
- Monitoring data sent to unauthorized and/or personal email addresses

In today's security landscape, a security breach is not a matter of "if" but "when." While risk tolerance is up to each individual organization, the way risk is managed is important, and there are definitely best practices to follow.

With increased regulatory pressure, and the cost involved, the financial services industry must carefully consider each investment decision and the impact it will have on the end consumer, regulatory requirements, and their bottom-line. The good news is that there are many opportunities for organizations to create win-win situations that improve customer interactions, preparedness, and resilience against security threats, while also helping to achieve long-term cost savings.

Michael O'Connor is SVP Service Delivery at Aspen Grove Solutions. Michael has over 18 years' experience delivering technology solutions. Over the last six years Michael has worked at Aspen Grove Solutions on the Aspen iFamily® suite of applications, providing a robust property management platform that is easy to use and quick to implement.

Here are six key components of any security policy.

1. Identification of organizational risks related to security
2. Establishment of security governance
3. Recognition of risks associated with remote access to client information
4. Evaluation of risks associated with vendors and other third parties
5. Policy, procedure, and oversight process development
6. Strategic plan for developing the capability to detect unauthorized activity