INDUSTRY INSIGHT / DARREN KRUK

A MEASURE OF SECURITY

With cyber-attacks looming as a real and ever-present threat, the mortgage services industry must instill security measures at every level of its everyday business.

One of the fastest-growing and fastest-changing professions is that of the security professional. In today's world, a security professional manages more than a business's physical and employee security. These professionals must be versed in information risk management, governance, compliance, IT processes, and increasingly possess depth of knowledge regarding cyber-security. The repercussions of cyber-attacks and the global nature of these threats have the potential to impact all industries, including the mortgage services industry. And cyber-attacks are unfortunately becoming the new business norm as such advances in technology, as mobile, cloud services, IP enabled workplaces, and social networking are adding to the layers of systems that need vigilant monitoring.

Although the core function of information security applies to all businesses, each industry has its own unique requirements and guidelines, in addition to the requirements and guidelines specific to the regulatory entities that oversee it. Mortgage companies and their field services partners fall under the information security regulatory requirements and guidelines of the Consumer Financial Protection Bureau (CFPB) and the Gramm-Leach-Bliley Act.

Almost every day there is a new report of a company that has fallen victim to a malicious cyber-attack, and these attacks are becoming increasingly more sophisticated. Recently, a large health care provider discovered it was the victim of a sophisticated hack, which affected not only its employees, but also more than 80 million accounts that were liberated from the company's databases. This breach, unlike the numerous others this past year, obtained personal identity data instead of payment card data seen in many of the recent retailer attacks.

How do businesses protect themselves from today's ever-changing environment, and more importantly, how does an information security

"Information security should be a welcome partner with the business functions of any organization. As such, it should be baked into business decisions from the onset. Do not think of it as just another cost of doing business, but rather a business initiative that provides service improvement and savings."

professional know whether the proper controls have been implemented and if the controls in place are sufficient?

KNOWING YOUR ASSETS

There are standard formulas that must be followed that apply the basic security management protocols, such as access control lists, secure firewalls, Intrusion Prevention Systems, segmentation, logging, and monitoring. But these are the mechanics of prevention. To fully understand the depth of a highly dynamic and complex information system, the information security team needs to first understand why they would be a target of a cyber-attack in the first place; what do they have that would attract a hacker? To understand this, the information security team needs to think like a hacker and take a hacker-centric approach to security. What are the points of interest? For most hackers their interest lies in a company's data and/or systems.

To understand what might be of value, a complete asset inventory is necessary. An asset, for example, can include such devices as computers, tablets, and smartphones. An asset can also include data and a company's physical operating system. Why would a hacker be interested in a system? Hackers are always looking to launch a hack from a better platform. A company may have minimal data, but their platform may entice a hacker.

Mobile technology is one of the biggest competitive advantages for many customer-facing businesses. Whether your customers are consumers or other businesses, being able to harness the power of mobile technology has become a game changer. For several years mortgage field services companies have been investing millions of dollars annually in mobile technology and applications to better meet growing client needs, as well as the needs of their inspectors and vendors.

Although field services companies cannot dictate which devices inspectors and vendors use to complete their assigned work in the field, they can require the use of only pre-approved, closed community applications that have been properly vetted and inventoried. Why is this important? We live in an interconnected world where business and personal time often overlap. One minute a tablet or smartphone could be used for work purposes, the next minute to send a personal email or access an external webpage. Without the proper controls in place, these devices can become a goldmine of information to exploit.

Millions of points of data are generated each and every day, but not all data is created equally. To fully track this data, it is vitally important to clearly define the classification, or rank, of each data element and create a matrix that qualifies where each data element resides. This is important because the level of protection provided is controlled by the predetermined ranking of the data element, as well as the level of risk the information poses if exposed. It is equally important to classify and track all data that is shared externally. For example, confidential information, such as loan numbers, are ranked the highest and require SSL encryption to the end point.

INTEGRATING INFORMATION SECURITY WITH BUSINESS

Information security should be a welcome partner with the business functions of any organization. As such, it should be baked into business decisions from the onset. Do not think of it as just another cost of doing business, but rather a business initiative that provides service improvement and savings. For example, by keeping anti-virus software up-to-date, new vulnerabilities will be addressed through routine security patches that "plug the holes." For mobile devices, this is especially true as new software versions and applications are continually introduced.

To be successful, information security should be an integral part of any organization's business culture. This integration starts at the top with executive ownership and support. Executive buy-in will help ensure the success of such internal undertakings as security and compliance advisory boards.

These boards can provide continuity of knowledge, leadership, executive oversight, and guidance for security and compliance policies and activities, and ensure ethical behavior within the organization.

RISK-BASED MODELING

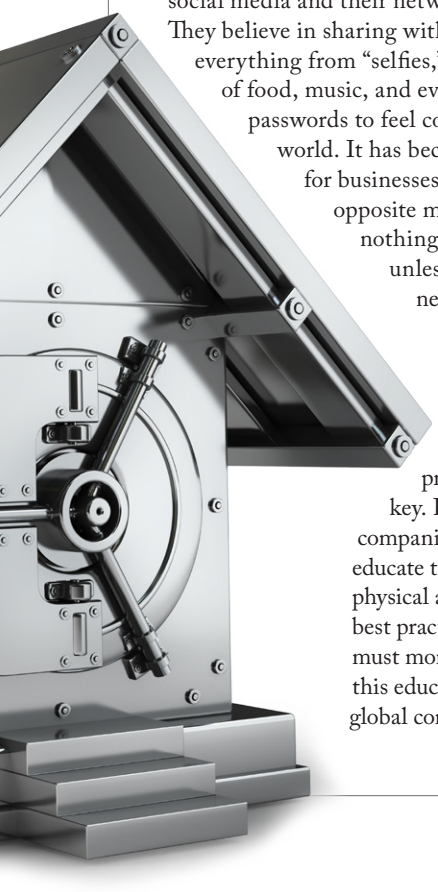
Taking a risk-based, or threat-modeling, approach to information security is important to effectively assess risk exposure and to determine how to best balance risk with action. Once the types of systems and data that exist have been classified, they can be rated according to their acceptable risk and threat levels. Risk-based modeling identifies the data and quantifies the risk of exposure, and the potential risk to

stakeholders should it be exposed.

Risks to your applications and systems need to be included in the risk-based modeling exercise as well. This includes email, file transfer systems, and storage systems that are susceptible to data loss. Email is such a universally used tool in daily business and personal interactions that it has gotten to the point where it has become innocuous. Not many think to take into consideration the risks associated with something as simple as sending an email with a file attached to a non-company system. However, one must consider how that data is transferred or stored on the other side. It might not be a risk worth taking.

CREATING A SECURITY-CENTRIC CULTURE

Building a holistic security culture is probably the hardest thing to do in a non-security based company. Our world has been forever changed by social media and its integration into daily life. The challenge is a common one in today's world—how do we change behavior to maintain privacy and to protect what is important in this over-sharing, ever-communicating cyber world? Next generation employees grew up with a cell phone in their hands, constantly tied to social media and their network of friends. They believe in sharing with one another everything from "selfies," to pictures of food, music, and even personal passwords to feel connected to the world. It has become a challenge for businesses to instill the exact opposite mentality—that nothing should be shared unless absolutely necessary.



Education and continuous information security awareness programs are key. Field services companies must not only educate their employees on physical and data security best practices, but they also must monitor and track this education to ensure global compliance and understanding. To ensure compliance in the field, inspector and vendor networks must be educated on these same industry best practices.

Ongoing information security education for everyone who has access to sensitive information is critical to ensure daily compliance with all information security protocols and applicable industry guidelines and requirements.

Routine monitoring and auditing of vendor networks can help identify gaps that need to be addressed and certify that anyone who has access to confidential information knows and practices the appropriate steps to protect it.

TESTING AND AUDITING

Testing and auditing can be the most important part of measuring your data security controls. And, with the renewed focus and investment on vendor oversight within the financial services industry; internal, external and, vendor network testing and auditing have become commonplace.

Regularly scheduled internal audits not only gauge the effectiveness of a data security strategy but can also point out areas of improvement and should be looked upon favorably. Field services companies typically receive and utilize confidential consumer data, and it is imperative that the security controls safeguarding this data are robust and comprehensive.

External audits should be viewed similarly. As regulations within the financial services industry continue to expand, ongoing third-party vendor audits have become routine. Part of this audit consists of an information security assessment in which a review of such protocols as physical security, application permission and authority levels, data integrity and protection (encryption), and network vulnerability are tested.

Much like the financial services industry, some field services companies have taken the audit process to the next level by implementing routine, on-site vendor audits as part of the overall audit protocol. A portion of this audit focuses on a vendor's data security compliance and frameworks. Routine monitoring and auditing of vendor networks can help identify security gaps so that anyone who has access to confidential information knows and practices the appropriate steps to protect it.

"Building a holistic security culture is probably the hardest thing to do in a non-security based company."

GAUGING SECURITY SUCCESS

Is there a measuring stick with which to gauge data security success? Some claim the ultimate measuring stick is not having been a victim of a cyber-attack. Unfortunately, that is a naive view of the information security world. A company cannot and should not claim success merely because it has not been the victim of a cyber-attack. The overall measure of a company's security framework is an amalgam of many different control principles. The field services industry has embraced and invested in the people and technology to meet the information security requirements head-on. It is one more way to strengthen the industry and provide clients with the security needed in this interconnected electronic business environment.