Bt-t
SPECIAL ROUNDTABLE SECTION
Financial Technology News and Strategies *www.banktt.com*

Addressing Insider Threats, Cyber Attacks & Data Security

As tired as it may sound, training is still the most important risk mitigation factor in reducing the number of insider threats. Insider threats originate either through the vulnerability of human kindness and the rush of our non-stop world, or through malicious and disgruntled actions.

With the majority of corporate training today being more of a checkmark for management then actual user education, employees have created ways to bypass the act of learning for sake of time. Requiring the review and acknowledgement of policies and possibly going through a slideshow presentation leads the majority of users to bypass the review, and click acknowledge.

Proper training should include Social Engineering examples relevant to your organization. Errors and omissions are still a large cause of downtime, service degradation, and financial loss. If your operations include entering values, alpha or numeric, work with development to design built-in checks and acknowledgement prior to submission, or for operational changes, ensure you have a Change Management procedure.

Users hear your directive that personal computers and storage devices should not be brought to the workplace, but also help them understand why and how their harmless flash drive could easily become infected and then spread malware throughout your environment as well as the costs and operational and strategic risks that come with.

* With the Venminder solution, you can:
* Perform a risk assessment on your vendor’s product/service
* Assess a vendor contract for compliance with FFIEC guidance
* Create oversight requirements for each vendor
* Set and complete oversight tasks
* Create executive and board level reports regarding vendor risk, your mitigation controls and results
* Use Venminder resources to analyze your vendors’ financial health, SOC report, BCP/Disaster recovery testing and Cybersecurity preparedness.

Breaches will continue to occur as long as humans are involved in ensuring the proper controls are in place and functioning. Be it an under-protected vendor portal or a simple email attachment, vulnerabilities as simple as these open the door for malicious actors. This is not to say that you should not protect your information assets, as defense-in-depth, the act of adding layers of security around your critical data may deter or slow an attack so that it is detectable.

Asset Management, knowing what data, applications, and systems are on your network and all of the connections that your network maintains and allows is a first step towards a more secure bank. Have you documented how each of your vendors connects to your network? Do you know the logical and physical location of sensitive data and the protections that surround it on your network? Are you responsible for protecting that data, or is your vendor? How will you know if you’ve been compromised if you don’t know about all of the systems and data on your network?

Vendor Systems will continue to be a target for cyber attacks because of the sheer volume of data available for thousands of banks and millions of customers stored in one location.

Your bank, like all others, has many vendors providing services that are critical to your operations such as your core, card processing, item processing, loan processing, etc. These vendors provide you with Service Organization Control (SOC) reports, but do you really know what the 150 pages are telling you about how they’re handling your data and managing your systems? Venminder will analyze your vendor’s SOC reports and provide a summary informing you of possible risks in your vendors’ controls. In addition, Venminder can also perform a deep dive into your vendors’ performance on Overall Information Security, Cybersecurity, as well as Business Continuity and Disaster Recovery reviews. Each of these reviews provides a unique insight into your vendor and the potential risks involved.

In addition, Venminder has an exciting new partnership with SecurityScorecard. SecurityScorecard continuously monitors all registered IP addresses for your vendor to detect real time vulnerabilities. The service will detect insecure open ports, leaked passwords, missing security patches and more.   With SecurityScorecard you no longer have to rely on out of date documentation, vendor answered questionnaires or expensive on-site visits.

venminder

Contact Info

www.venminder.com
(270) 506-5140

Aaron Kirkpatrick, CISSP
Information Security Officer

Aaron Kirkpatrick is an Information Security Officer at Venminder where he leads a team in security and compliance analysis. Aaron works with financial institution clients to help answer the ever growing challenges and regulatory demand for vendor management compliance by performing reviews of their vendors SOC Reports, Business Continuity and Disaster Recovery & Avoidance Plans, Cybersecurity Risk and Information Security. Aaron has a background of Governance, Risk and Compliance roles in financial services and data center companies, as well as being a network security instructor for a local college. Aaron earned a Bachelor’s of Science in Management Information Systems from Iowa State University and an AAS in Network Administration and Engineering.