MICRO FOCUS

Flash Point Paper
Security

Staying Ahead of the Financial Security Compliance Curve

As government regulators evolve their mandates and the bar for consumer trust continue to rise, effective security is often a top priority. To meet these demands, security must be more than just check box across the organization.

When it comes to information security and privacy in the financial industry, expectations are high. Not only are government regulators scrutinizing businesses operating in this industry, consumer expectations are increasing as well. From the largest of the banks to small investment advisors—and all the financial-focused organizations in between—security has to be a top priority. Instead of just a product or a process, security must be ingrained into the culture and philosophy at the most complex levels of business operations. When properly executed, information security programs can serve as competitive differentiators and help businesses with numerous compliance requirements.

Fifty-one percent of respondents to the Accenture 2017 Compliance Risk Study forecast information security risk to be among the top three most challenging areas to manage within three years' time. Perhaps finance and legal aside, managing security is one of the most difficult things business leaders must contend with. Whether it's PCI DSS, the Gramm-Leach-Bliley Act, or any future regulations that mandate protective measures over financial related systems and information, it's clear that compliance has to be a top priority. I'm not talking about the checkbox type of compliance that businesses in other industries tend to focus on. Instead, there are numerous security controls that must be ingrained within the IT function as well as the overall culture of the business in order to establish true governance. An effective information security program that lends itself to positive outcomes in the compliance department must include:

- Ongoing risk assessments that look at both sides of security: technical and operational
- Reasonable policies and procedures that are enforced/implemented with the proper technologies
- Identity and access management processes and technologies that work to enable the business rather than get in the way
- Real-time system monitoring and alerting
- Resilient systems that can withstand outages or be promptly recovered
- Incident response procedures including breach notification steps for when the worst-case scenario does occur

5 Things to Do for Better Cybersecurity:

Don't tell yourself that you're too small to be a target

- *Level set with a third-party audit*
- *Perform periodical training for your staff*
- *Avoid applications with incomplete security*
- *Make sure your protocols are up-to-date*

In my work as an independent information security consultant, I often see people taking the wrong approach to the industry and government regulatory requirements. The biggest mistake is overconfidence. Many people are unrealistic when filling out those security self-assessments. They also over-rely on paperwork (security policies) that's not enforceable or enforced for much of their security. Sometimes it's management assuming all is well because IT and security staff are busy and spending a lot of money. Sometimes compliance officers and internal audit staff are not looking in the right areas to find the true security posture of the network environment. I've even seen IT and security professionals go about their work under the assumption that legal counsel and management are capable of minimizing security related risks through their paperwork and cyber insurance policies. What's really taking place is something called bystander apathy. Everybody assumes that everyone else is carrying their own weight. At quick glance, it looks like security is in check but, in reality, security controls are siloed and there's no cohesive oversight. Given the number of people involved and level of complexity associated with these aspects of security, gaps such as these can be particularly problematic in the areas of risk assessment, access management, and incident response. And when these areas are not well-run, compliance suffers.

Instead, true compliance for financial institutions requires a deep understanding of existing risks combined with well-executed security initiatives (products, processes and the like) that have the ongoing support of the highest levels of management. One thing you cannot forget is that compliance does not equal security. Many people think that it does, including consumers. The reality is that it never has, and it never will. Still, many people tend to take that approach to managing their information security-related risks. From the consumer's perspective, when they see things such as security and privacy policies combined with technical controls that appear to lockdown their online experience, it's easy to assume that all is well. It's often not.

I think financial industry compliance as we know it will continue to evolve, especially in terms of accountability. As consumers become more tech-savvy and end up expecting more out of their financial institutions, we will witness a trickle-up effect that pushes businesses operating in this industry to do more and do it better and faster than ever before. I suspect the regulators will further tighten down on their audits and enforcement. With today's complex network and application environments, this is going to require centralized control that can help reduce network and security complexity and maximize visibility. This is especially true for today's more complicated network environments that incorporate traditional computer systems with newer mobile devices, cloud applications, and Internet of Things devices.

Truly locking down security while maintaining usability is not going to be easy but it can be done. It takes good foresight and planning and, perhaps most importantly, common sense. Stay connected to the rules and the solutions in the security marketplace. Don't get too caught in "compliance". Instead, focus on the larger goal of establishing and maintaining a resilient financial systems environment and the results will take care of themselves.

To learn more about Micro Focus® Solutions visit: **www.netiq.com/solutions/identity-access-management/**

Kevin Beaver is an independent information security consultant, writer, professional speaker, and expert witness with Atlanta-based Principle Logic, LLC. With over three decades of experience in the industry, Kevin specializes in performing independent security assessments and consulting to help his clients uncheck the boxes that keep creating a false sense of security. He has authored/co-authored 12 books on information security including the best-selling Hacking For Dummies and The Practical Guide to HIPAA Privacy and Security Compliance. In addition, he's the creator of the Security On Wheels information security audio books and blog providing security learning for IT professionals on the go. Kevin can be reached at through his website at **www.principlelogic.com** and you can follow him on Twitter at **@kevinbeaver**.

Contact us at:
www.microfocus.com