Building Resilience through Digital Risk Management

As organizations undergo digital transformation and increasingly depend on internet-connected devices, disruption occurs. With that disruption comes risk. ***Steve Schmalz****, Field CTO for RSA's Federal Group, discusses digital risk management and key components of resilience.*

What's the biggest challenge of protecting an ever-expanding perimeter?

Visibility. That means knowing what's happening on your networks and who is doing what — regardless of the device or service being used. It means being able to monitor endpoints, keep track of logs, look for potential problems, ensure all policies are enforced and so on. The amount of real estate to be monitored keeps expanding. It's not just the number of things you have to look at, but the complexity of those new devices and the new ways of doing business.

Please discuss an integrated risk management approach to cybersecurity.

A core component of the NIST Cybersecurity Framework, which aligns with RSA's risk management approach, is visibility. You have to understand your cybersecurity posture — what controls you have in place and what threats are out there. Based on that analysis, you implement the ability to monitor that continuing state and identify the real threats to your organization. Some things are extremely important to protect and some aren't. As you identify threats and their targets, you can start calculating the risks and putting dollar amounts on them. Then you develop a plan for modifying your existing controls and processes to meet those evolving threats and to reduce those risks. It's a continuous process of assessment and refinement that should be integrated across the entire organization, not just within cybersecurity.

What can cybersecurity leaders do to adapt their security operations centers (SOCs) to the changing landscape?

SOCs typically have monitored network traffic and endpoints. They are at the center of that visibility process we're talking about. It's critical that the modern SOC extends monitoring functionality out to the Internet of Things as well as cloud-based resources. Besides monitoring all of that real estate, the SOC itself should take advantage of any cloud infrastructure that is in place. As the COVID-19 pandemic evolves, SOC analysts must be able to access their tools and dig into incidents from a secure connection at home as easily as when they sit in a SOC. Without that, it's going to be hard to maintain a sound cybersecurity posture.

As multifactor authentication becomes a more important tool for workforce transformation, what do organizations need to consider?

Flexibility and usability are at the top of the list. It's important that you can provide the type of authentication that's most appropriate for the individual and the resources they're attempting to access. In addition, if authentication isn't simple to use, people will find a way to get around it. Workers often become your worst threat because even though their intentions are good, their hack can open up holes for malicious actors to follow.

How can organizations build resilience into their security strategies so they are best prepared for any disruption?

Planning ahead for how you'll address problems and putting contingency plans down on paper is an important risk management process. Organizations need good security workflows and a way to aggregate information about their networks, valuable resources and who is doing what in the organization. Then they need plans for triaging the most devastating risks first. It's impossible to think of every threat, but organizations can start by considering what types of incidents could interfere with critical capabilities and prevent them from completing their mission. With that information, organizations can put together contingency plans, even when they're not quite sure what potential threat might bring about that particular loss of functionality.

What are some unexpected consequences of the pandemic on security and risk management?

Initially, organizations were in a rush to find the appropriate way to extend the use of their existing authentication or access management technology to SOC staff and other people working from home. They got that low-hanging fruit to make things more secure, but now they're struggling to manage their SOC, do governance and keep security workflows in place. It's also more difficult to do some everyday security jobs. In terms of innovation, the pandemic accelerated the use of the cell phone as an authenticator. A lot of people were doing this already, but the pandemic certainly pushed this wave of mobile-centric access to sensitive resources.

Detect and respond to threats **your way**

With complete visibility, analytics and automated response

Tap into your full potential as a threat hunter with RSA NetWitness® Platform. Our industry-leading evolved SIEM and threat defense platform gives you all the capabilities you need to detect virtually any threat anywhere: end-to-end visibility across your entire IT infrastructure, advanced behavioral analytics and automated response. **Be the threat hunter you're meant to be.**

Go ahead.
Be you.

RSA

RSA NETWITNESS® PLATFORM

Learn more at rsa.com/publicsector