MANAGING CYBER SECURITY RISK IN CORPORATE NETWORKS

A Perspective on Maintaining Resiliancy

Can the resiliency of a business[1] be quantified? Some say that is impossible to pin down. Temporarily side-stepping that debate, APQC caught up with two experts who maintain that in the realm of cyber security—with its constant vigilance and rapidly shifting dynamics—organizations should gauge their ability to withstand a threat to their digital networks in concrete terms. The key lays in tracking the organization's digital resiliency on a daily basis, which can boost compliance and improve incident response.

APQC's Mary Driscoll, the senior research fellow for financial management, recently spoke with leaders from cyber security firm RedSeal Inc. about their approach to providing a metric of digital resilience. Ray Rothrock and Steve Timmerman stressed the notion of gauging IT network risk and prompting conversations among senior executives about this critical dimension of enterprise risk management.

Note: APQC does not review or endorse any technology-based solutions to business problems. Our role here is simply to illuminate questions and encourage further study.

Ray Rothrock is RedSeal's chairman and CEO. Previously, he was a general partner at Venrock, one of RedSeal's founding investors. Rothrock participated in the White House Summit on Cybersecurity held at Stanford University in February 2015.

Steve Timmerman is RedSeal's vice president of business development. Timmerman has served as the vice president of marketing at ASSIA Inc., ShoreTel Inc., and Proxim Wireless Corp.

APQC: What about network security has recently shifted for organizations?

RR: As a venture capitalist, I have been working on cyber security since the Internet was invented. I have seen the technology, threats, and solutions evolve. And I think we're now in a new era. This is the third era when the best prevention and protection systems are no longer capable of keeping the bad guys out. You see it practically every week in the newspaper.

It's not because people don't know how to run their security systems. It's not because they have bad products. It's not because they've done anything wrong. The bad guys have figured out how

[1] According to www.techtarget.com, business resilience is the ability an organization has to quickly adapt to disruptions while maintaining continuous business operations and safeguarding people, assets and overall brand equity.

©2016 APQC. ALL RIGHTS RESERVED

to engineer attacks that get inside the network. Therefore, the corporation—the digital enterprise—is faced with a new threat. That is the threat that resilience can address.

What is resilience? Resilience is the capability to withstand and operate right through a threat or an actual incident. Unfortunately, networks aren't built with resilience in mind at all. There is very little resilience in a modern digital network.

What do I mean by that? In your typical large-corporate network are hundreds, thousands, or hundreds of thousands of different devices from more than 100 different vendors. They all do a specific function. They all have a configuration piece of software in them, and they interoperate. Our software reads those configuration files out of those devices, and we load it into our enterprise software, which builds a software model.

That model is not unlike a very sophisticated spreadsheet that's full of formulas. If you change something in Cell B-25, it might affect what went on in Cell D-18. Likewise, if we change a router in Spokane, Washington, and if my network model is updated while I'm monitoring that network from elsewhere, I can see that change in real time and the impact that it has in terms of the network's risk exposure.

A lot of security products deal with specific elements of the network such as the firewall or the host. But I believe what you need is an overview of the entire network—and a judgment about how resilient your entire network is, not just the parts. You need the diagnostics, intelligence, and the capability to use that model to play war games with it, to conduct penetration testing against the entire network, and to optimize existing cyber investments.

APQC: Can you provide an example of how the platform works?

RR: The chief security officer requests $100 million from the CFO to fix the enterprise network. The CFO will ask: How will you prove that it works and that you won't need another $100 million next year?

We have taken that incredibly complex analysis down to a single score. We call it a digital resilience score. It is modeled after personal credit scores. Like the well-known FICO score, it's on a scale from 300 to 850, and we trend it over time with three non-technical components.

Say the CFO sees a score of 450. The chief security officer wants $100 million to raise the resilience score to 600. Before the CFO spends the money, she can model it and see what happens, in terms of a judgment that a C-suite member can understand.

ST: Typically, a chief security officer would request an investment in input terms such as 500 more firewalls, 300 antivirus packages, and 25 fire intrusion detection systems. What senior management executives need is the ability to see the potential outcome and a practical way to talk about that outcome.

APQC: How is this going to help a CFO or senior enterprise risk officer assure the board of directors that a particular risk is well managed?

©2016 APQC. ALL RIGHTS RESERVED

RR: Think, first, about what the C-suite does not need: a list of investments in security products. Would you buy a building that doesn't have a fire prevention system in it? Of course you wouldn't. That's a higher risk for you. But, back to the corporate digital network, looking at a list of security products does not give you an assessment of that network's digital resilience.

Consider an example where your organization has a score of 650. You assess the network of an organization you're going to acquire and find a score of 475. You're buying a network that is riskier than yours. Undoubtedly, when you connect to it, your score will drop and that might not be acceptable. Even if you proceed with the connection, you're going to renegotiate price and add new liability escrow elements.

APQC: So organizations are using this in the due diligence phase to assess the viability of an acquisition?

RR: It has been used in the financial services arena in that strategic context. But on a day-to-day basis, the digital resilience score is mostly used by the operational leaders because they're making changes to the network constantly.

APQC: And this could help to manage risk in corporate payment systems?

RR: A number of electronics companies use RedSeal in their supply chains. They demand that their suppliers run it to confirm a secure environment. Everything is connected. You're as risky as the most risky element of your supply chain.

ST: The Target example started with an HVAC vendor that was compromised and had access to the corporate network that wasn't properly segmented from the point of sale system, and we all know how that story ended. It's not enough to lock down your own network. You have to be able to certify any part of your supply chain that accesses your network or that you do important transactions with.

RR: Sony is another example. They had 6,000 suppliers on their network. After rebuilding their network in the wake of their security breach, they now require a full risk assessment of any supplier. They've pushed that out into their supply chain because there is a lot of intellectual property that moves around digitally in a place like Sony.

APQC: Are there any government applications that you see?

RR: We have about 230 customers, a third of which are government agencies. We're in every branch of the military service, the civilian agencies, and the intelligence agencies.

As an example, we're working with a multi-billion-dollar government enterprise with a network that is completely outsourced. They look at the digital resilience score to know whether the network is getting better or worse. A service level agreement is in place for the provider to bring the network up to certain levels over certain periods of time.

©2016 APQC. ALL RIGHTS RESERVED

APQC: How does this roll up into a management dashboard?

RR: Our dashboard has not only management information but also trending and technical information so that an engineer can dispatch a service ticket or whatever. Our key dashboard is in the smartphone app.

APQC: How does it go deeper? How does it prioritize your vulnerabilities?

RR: It's giving you not only a raw list of those vulnerability scores but also the network context: the situational awareness. You could have two computers with the same exact vulnerability score that other products provide. If one of those was in the Fort Knox of your network and well-segmented, and the other one wasn't, that presents two different vulnerabilities of your network, even though they have the same score. They provide a different situational risk to your business. That is the kind of prioritization we do.

APQC: What are the key questions risk officers need to ask in order to expand the conversation about security protection to the bigger picture you're looking at?

RR: First, what audit policies do you have in place? What confirmation can you give me that those policies are in force and that they're not changing? Networks are dynamic, so oftentimes policies are violated quickly.

Second, can you convince me that you understand your network? Do you have a comprehensive capability of managing your digital enterprise from a risk point of view?

Third, what are you paying for cyber insurance? We project that our digital resilience score could actually lower premiums.

ST: Cyber insurance is in the "Wild West" stages right now. Insurance companies have been asked by their current clients to provide cyber insurance. These insurance companies are figuring out what actuarial data to collect and how to correlate risk across a portfolio.

So, insurance companies have been writing very low-coverage policies with high premiums and a lot of terms and conditions to exclude all of the things that you really care about. We think the core problem is just a lack of information.

If I can demonstrate I have a higher digital resilience score and that I pay attention to how I've architected my network, how I've segmented it, how I've prioritized tasks and addressed those, then that should make me a lower risk and give me a lower premium.

As we talk to the more savvy companies on this topic, this has become a C-level and a board-level issue. There should be a cyber security executive on the board, just like you have for audit, compensation, or any key areas. If you make this only an annual conversation with the board, the company could be hacked and put out of business in that cycle.

©2016 APQC. ALL RIGHTS RESERVED

ABOUT APQC

APQC helps organizations work smarter, faster, and with greater confidence. It is the world's foremost authority in benchmarking, best practices, process and performance improvement, and knowledge management. APQC's unique structure as a member-based nonprofit makes it a differentiator in the marketplace. APQC partners with more than 500 member organizations worldwide in all industries. With more than 40 years of experience, APQC remains the world's leader in transforming organizations. Visit us at www.apqc.org, and learn how you can make best practices your practices.

©2016 APQC. ALL RIGHTS RESERVED