Why Improved Recovery From Cyber Incidents Is Critical

Optiv’s Jessica Hetrick Discusses the Need to Focus on Recovery and Resiliency
Continuing ransomware trends are making it increasingly important for organizations to proactively and comprehensively consider what cyber recovery means, says Jessica Hetrick, cyber resilience leader at Optiv.

When an entity suffers a ransomware attack affecting the company’s ability to operate, “It’s not just a cybersecurity problem; it’s a business problem,” she says.

This is fueling the need for entities to not just understand what their technology interdependencies are across the business but also understand how to protect them, she says.

In a video interview with Information Security Media Group at RSA Conference 2022, Hetrick also discusses:

- The risks, threats and impacts clients face
- Questions security leaders should be asking about their own enterprise’s abilities to recover and be resilient
- Components and goals of Optiv’s Cyber Recovery Solution

**Current Risks and Threats**

**MATHEW SCHWARTZ:** What are some of the risks, threats and impacts that your customers face today?

**JESSICA HETRICK:** As the cyber advisory solutions leader, Optiv sees a lot. We are a major cyber partner for organizations in terms of how to better secure them. Overall, the biggest threat right now – and I think
this trend will continue, especially with COVID now in semi-rear sight – is ransomware. Both small and large organizations are getting hit by financially motivated crimes. As that trend continues, we also see a big risk to organizations and their ability to trust their technology that’s in place. So organizations need to be not only thinking proactively, but understanding what preparedness means – both for driving down the risk of if something occurs and for when something occurs, and knowing that “when” is inevitable. If the adversary wants to get in, they will. A lot of organizations right now are looking at taking a proactive step in the recovery space.

The Need for a Cyber Recovery Solution

SCHWARTZ: Why do organizations need a cyber recovery solution?

HETRICK: That proactive thinking needs to spread throughout the organization. Technology does not just impact the security space anymore. If you have ransomware in your organization, not just one part of the business goes down. It’s not just a cybersecurity problem; it’s a business problem. A cyber recovery solution helps organizations think holistically about what recovery means so they can proactively understand the criticality of assets within the environment, and from the systems, data and applications – all of the interdependencies across the business. We partner with organizations to not just understand what those interdependencies are, but subsequently to understand how they can better be protected. We think proactively about recovery, which supports the identification prioritization across the environment of critical components.

Solution Components

SCHWARTZ: What are some of the components of the cyber recovery solution?

HETRICK: In the traditional BCDR sense, organizations are categorizing what’s most critical within the environment. However, those programs don’t tend to take the technology recovery piece into account because of natural disasters coming as the priority in past times. The cyber recovery solution partners with these BCDR programs. We look at the identification and prioritization of not only critical assets but general processes. And then we help map out all of those critical dependencies where we see systems need to be recovered first, before applications are brought online. BCDR programs might look at applications and tier those out, but then they’re not looking at the whole holistic business picture.

“Both small and large organizations are getting hit by financially motivated crimes...organizations need to be not only thinking proactively, but understanding what preparedness means.”
We work across the business from the technology perspective, but we also map everything out with the different system owners, data owners and application owners. We also help support the implementation of an air-gapped immutable vaulted technology – the cutting-edge components that interweave with the people and the processes. And the final major component of the cyber recovery solution is that we help organizations test those different components that we put into play. We help them understand how people respond to different things, what recovery actually looks like, and how their systems, data and applications all interact to holistically recover to a secure state.

**SCHWARTZ:** Is one of the goals to have some assurance that things are going to behave the way that you hope and have planned that they will behave?

**HETRICK:** Yes, and to account for the adjustments in the environment. Sometimes, things might change. Every complex system out there changes on a daily, if not hourly, basis, so taking into account those adjustments is a necessary piece to understand, at the granular level, how things interact, including the people. Our process allows for all of those different components to come together so organizations can recover holistically.

**Solution Components**

**SCHWARTZ:** To what degree is customization required, and how do you help organizations do that?

**HETRICK:** Customization is imperative. Every single aspect of the cyber recovery solution is customized to the environment. From a prioritization perspective, the front-end process might be more important. Different things are important to different industries. Finances tend to be up there for organizations – their ability to pay people or their ability to do transactional business. But everything after that front-end process comes into the customization perspective, from naming those individual systems at a granular level to identifying the interdependencies that are unique to the organization. We approach customization with very systematic methodology.

**Communication Tactics**

**SCHWARTZ:** What tactics should security leaders use when they’re attempting to communicate with business leaders about how this addresses risk or resiliency?

**HETRICK:** Organizations need to understand what their business is doing. Having security professionals partner with the business is becoming an increasing need. And overall, risk reduction is the most understood form of that communication. General best practice is to understand how it quantifies in the environment and where it would take priority. Organizations that are more immature might see BCDR as the central component, but then they don’t take into account the fact that ransomware might hit an environment and how they would recover from that. I recommend that organizations understand what the threat landscape looks like in terms of not only their industry, but their specific organization, and then understand ultimately where the cyber recovery solution fits into that.

They need to know how much they rely on technology to do their business or to enable their business. The most successful communication
“Having an air-gapped immutable vaulted technology in place and understanding the process to recovery from that is imperative for organizations in order to understand what a secure state looks like and ultimately reduce the risk of downtime.”

happens when organizations take into account the technology components coupled with the threat landscape to communicate the risk overall, and also what the cyber recovery solution does to reduce that. All of those pieces together create a general standard risk practice. Then organizations need to quantify that a little bit more and drill into the specifics of what they do and don’t have.

Advice for Security Leaders

SCHWARTZ: When you work with organizations, what other questions do you tell security leaders they should be asking about this?

HETRICK: I emphasize that the cyber recovery solution, while focused in the recovery space, supports a much broader business objective, which is risk reduction as a whole. Optiv’s cyber recovery capability doesn’t just take into account the different systems, data and applications and how they all are interdependent. We also identify systems that organizations didn’t account for before. So from an identification and prioritization perspective, they’re able to spearhead the preparedness in those spaces as well, which gives them the ability to respond more rapidly. In the systems they had not previously accounted for, they can now flag intellectual property areas or any type of PII, or personally identifiable information, that might be in the environment that they didn’t see before.

I implore organizations to not only map out their environments from a network architecture perspective but to understand what the recovery systematic process is. That step-by-step build allows organizations to see what needs to happen first, second and third in their environment in order to securely recover. In a past life, I’ve seen what ransomware can do, especially if you don’t have secure backups or you don’t understand that the legacy replicated and redundant backups are what adversaries are targeting first. Having an air-gapped immutable vaulted technology in place and understanding the process to recovery from that is imperative for organizations in order to understand what a secure state looks like and ultimately reduce the risk of downtime.
As the cyber advisory and solutions leader, we manage cyber risk so you can secure your full potential.

Click here to learn more: www.optiv.com
About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

(800) 944-0401 • sales@ismg.io