RANSOMWARE RESILIENCE SUMMIT EUROPE

Benchmarking ransomware resilience and business continuity planning

Q&A: JEN ELLIS, VICE PRESIDENT, COMMUNITY AND PUBLIC AFFAIRS, RAPID7 AND CO-CHAIR, RANSOMWARE TASK FORCE

Kisaco Research

Jen Ellis

As vice president of community and public affairs at Rapid7, Jen Ellis is focused on advancing cybersecurity by building collaboration between the security community and those outside it. Most recently, she has been very focused on advocating strategies for deterring and disrupting the ransomware ecosystem, as well as helping organisations better prepare for, and respond to, ransomware attacks. Jen has extensive experience in managing crisis response, both internally for Rapid7 and previous employers, and externally as a crisis communications consultant for various third-party clients. She has worked in reputation and brand management for more than 15 years, always with a strong emphasis on building credibility, authenticity, and customer trust. She is a co-chair on the Ransomware Task Force, a non-resident senior fellow of the Atlantic Council, sits on the boards of the Center for Cybersecurity Policy and Law, I Am The Cavalry, and the Aerospace Village, and is a member of the board of advisors for the CyberPeace Institute and the Global Cyber Alliance. She has testified before U.S. Congress and spoken at numerous security or business conferences.

Jen Ellis
Vice President, Community & Public Affairs, **Rapid7** and Co-Chair, **Ransomware Task Force**

You were part of the Ransomware Task Force and fundamental to the 'combatting ransomware' report. What have you seen change since the report has been released?

Shortly after the Ransomware Task Force report was released, we saw a spate of high profile attacks against large critical infrastructure providers - Colonial Pipeline, HSE, JBS - which highlighted the impact of these attacks on society and the economy. Fuel being unavailable in multiple US states, hospitals closing across Ireland, and the cost of food staples increasing in numerous countries made it clear that ransomware attacks can create profound impact on our way of life and should be treated as a matter of national security.

Since then, we have seen the US' President Biden speak publicly about ransomware multiple times, even directly addressing the issue with Russia's President Putin. We've seen a concerted whole-of government effort to address the issue in the US, including the introduction of new Treasury sanctions, prioritisation of ransomware cases for law enforcement, public-private collaboration, and a greater focus on international government and law enforcement cooperation. There is also a great deal of government scrutiny on the role of cryptocurrencies, cyber insurance, private sector critical infrastructure providers, digital service providers, and sector regulators. There has also been a policy push towards greater transparency and reporting around cyber incidents and ransom payments.

One of the 'goals' laid out in the report was to 'disrupt the ransomware business model and decrease criminal profits'. There's been some high profile arrests and law enforcement announcements in recent weeks but overall, ransomware continues to

be very profitable for criminals. Do you believe businesses and other organisations are giving the threat of ransomware the focus it deserves?

Despite the many ransomware-related headlines, we still face an awareness and understanding problem around ransomware and cybercrime as a whole. Many organisational leaders don't recognise that the threat is relevant to their organisation until it's too late and they are left scrambling to respond to an attack. We continue to see cybersecurity being treated as a niche capability in too many organisations that fail to understand how reliant their operations are on connected technologies that can be disrupted by malicious actors. As a result, it is too often under-resourced, under-funded, or sidelined, leaving the organisation exposed to serious risk.

On top of that, even organisations that are investing and bought in on the need for cybersecurity are struggling with the increasing complexity of technical ecosystems, the interdependence of supply chains, the pace of innovation, and the various other odds stacked against them. Building a comprehensive defence-in-depth program is not straight forward, quick, or easy and we must stop talking as if it is. We need to make a fundamental shift towards focusing more on building security inherently into systems and processes, and integrating it broadly across any technology-dependent organisation.

Any organisation can fall victim to ransomware, creating catastrophic disruption for the organisation and those it serves. Are organisations communicating enough with each other to share best practices, lessons learned and insights?

Information sharing in cybersecurity has improved and become more commonplace over recent years, but we still have a long way to go. Ransomware incidents in particular are heavily underreported, which makes it hard to understand the true scale and dimensions of the issue. Organisations can certainly benefit from more openness. More information sharing helps destigmatize being a victim of an attack, and helps other organisations in the same sector, geography, or business size recognise that they too could become a victim. More information sharing on attacker trends also helps organisations build appropriate defences and alarms, and helps governments and others better disrupt attackers.

> “Ransomware incidents in particular are heavily underreported.”

You'll be talking at next year's Ransomware Resilience Summit series on 'determining roles and responsibilities in a response'. How critical is it for the business to pre-determine their responses and responsibilities to an attack before it happens?

The best piece of advice I can offer is not to wait until you get hit. Build a response plan now; identify your response team and their roles; explore your decision-making criteria and expectations; investigate whether you have capabilities in place to respond - for example, do you have regular offline backups? Do you know what your corporate point of view is on involving law enforcement? Do you know whether there are any regulations that would require specific actions? Do you have expert legal counsel to help you navigate those questions? Do you have a relationship with an incident response firm? Do you have cyber insurance, and if so, what does it cover? What is your corporate position on paying ransoms?

Cyber incidents, like any other crisis situation, are dynamic and will always offer unexpected challenges, but the better prepared you are in advance, the better able you will be to adapt and respond appropriately. And remember to have offline copies of your incident response plan available for all core responders.

The Ransomware Resilience Summit series will be held behind closed doors and under Chatham House rules to encourage the sharing of information, lessons learned and best practices amongst industry experts. How important do you think this is to winning the battle against ransomware?

It's important to create safe spaces where people feel comfortable sharing their experiences and insights, and asking questions. This kind of open discourse helps us better explore the current status quo, and understand challenges that reduce adoption or efficacy of preventative measures so we can start to frame better solutions. Candid information sharing also helps us investigate opportunities for disruption and deterrence of ransomware attacks.

What are you most looking forward to by being a part of the Ransomware Resilience Summit series?

I'm very much looking forward to hearing about the experience and insights of others at the Ransomware Resilience Summit, particularly attendees who are struggling to respond to the threat. I always hope that these events will reach people who are not already super expert on the topic, and will give them an opportunity to ask questions and learn. Those are the people I hope to meet at the event.

> **“It's important to create safe spaces where people feel comfortable sharing their experiences and insights”**

PRODUCED BY: Kisaco Research