Ransomware: Addressing the rising threat

The APAC Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "Ransomware: Addressing the Rising Threat," on November 10, 2020. CISOs from the Asia/Pacific region examined best practices in preparing for and responding to ransomware demands in an increasingly dynamic threat landscape.

Ransomware is not new, but it is evolving. Previously, when bad actors took control of a system and encrypted it, they would demand a ransom in order to get the system back. Now, however, they are casting a wider net, attempting Distributed Denials of Service (DDoS) that can entirely disrupt enterprise operations. Bad actors are also having success taking data, publicly announcing what they have taken and requiring a ransom for its return—with no guarantee the exfiltrated data won't be sold despite the payment of the ransom.

In this threat landscape APAC CISOs are asking important questions. How should we prepare for ransomware attacks? What are the pros and cons of paying a ransom? What should the CISO's priorities be after an attack?

Our speakers included Accenture Security subject-matter experts, a cybersecurity legal expert and peer CISOs. The session was hosted by Andy Vautier, Accenture CISO and ACF chair, and Andrew McLauchlan, APAC Lead, Accenture Security.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers or participants is revealed.

Why ransomware attacks are on the rise

Accenture's *2020 Cyber Threatscape Report* highlights the rise of ransomware as a major criminal enterprise: "A combination of emboldened threat actors earning large sums of money enabling them to invest and improve their operations, and a general weakening of organizational security, due to, among others, mistakes made as a result of increased stress, loss of staff and income, and a larger attack surface caused by increased remote working, can only serve to make things worse for businesses in the short term."

Some estimate that a ransomware attack occurs somewhere in the world every 40 seconds. Other experts report estimates as high as $19 billion in recent ransomware payments. Several factors contribute to this troubling trend. Threat actors and using off-the-shelf tools and demanding digital currency payments, thus making identification more difficult.

The return on their investment is increasing. They are threatening major disruptions, such as a Distributed Denials of Service (DDoS), and demanding significantly higher ransoms in return. They are becoming increasingly sophisticated, operating at an industrial scale with command-and-control techniques to leverage the capabilities of other rogue actors.

Cyber criminals are also getting more precise in valuing their attacks. They are accessing enterprise privacy policies and other documentation (i.e. revenue, cyber insurance policies) to calculate the perceived value of data and set their ransomware demands accordingly.

The World Economic Forum Advisory Board of the Centre for Cybersecurity predicts that ransomware attacks will proliferate and be deployed by smaller and less resourceful criminal networks due to the potential for high profit at low risk. Ransomware-as-a-Service will also grow and techniques like fileless attacks will most likely increase. The World Economic Forum also notes that the broader attack surface established in response to the COVID-19 pandemic (i.e. working from home, insecure networks) makes ransomware attacks more attractive.

Catching criminals is a huge challenge. The World Economic Forum notes that criminal networks can operate ransomware operations from a country and never violate its penal code by deploying malware from bots outside the criminal's host-country. They avoid detection by channeling ransomware proceeds via digital currency that are cashed out outside the host country and by never attacking victims inside the host country. This normally prevents host state law enforcement from investigating crimes on their own initiative. *Letters rogatory*—a formal request from a court to a foreign court for some type of judicial assistance—may be difficult to obtain given geopolitical tensions. Criminal networks take advantage of this situation which makes ransomware operations almost risk-free.

APAC CISOs confront the threat

One APAC CISO said that ransomware was #1 and #3 on his list of topics he recently presented to his board. Others shared detailed stories about recent attacks and said that supply chain partners are an attractive attack target. Threat actors are deploying a "spray and pray" strategy, testing third-party vulnerabilities as a pathway to their ultimate target.

CISOs are trying to keep their response playbooks on pace with an evolving threat landscape but no one can claim they are immune from a ransomware attack. Criminals are moving laterally across networks to do maximum damage. They are using penetration testing and signature-based detection tools more thoughtfully. And, in the extended environments enterprises are working in given the COVID-19 disruption, the increase in endpoints poses its own unique challenges.

Best practices

CISOs and subject matter experts who have overcome ransomware attacks point to best practices for preparation, remediation and recovery:

- Conduct robust pay/no pay ransomware scenario fire drills. “Ransomware attacks require business decisions. You can avoid panic by getting the Board and senior leadership to address the important questions before an event occurs,” said a CISO. Another CISO discussed the importance of simulating drills that put real pressure on the team, including Legal and Communications. Consider establishing a “Ransomware Task Force” to plan for and practice responses to ransomware demands.
- When attacked, keep the focus on recovery, not finger-pointing. The Board may want to understand why defenses were inadequate. Third-party providers and business leads may want to assign, or deflect, blame. “There will be plenty of time for second-guessing after an event but we have to keep everyone focused on restoration,” said a CISO. Enterprises generally aren’t faulted for having an incident, but for how they respond.
- “Don’t let a crisis go to waste.” A CISO said that a DDoS attack created an opportunity for business units and recent acquisition to “come clean” about systems and apps that had previously been shielded from the CISO. Simplifying the computing environment can reduce the attack surface.
- Don’t underestimate the resources required. “In the event of a DDoS attack you’ll need more resources to recover than you ever imagined,” said a CISO whose enterprise was shut down by bad actors. Include a resilient resource strategy in the response plan so you know where those resources are coming from.
- Don’t panic. “Learn to lean on the expertise of others,” said a CISO. Other CISOs reinforced the value of trusted relationships with their third-party response resources. That trust is built on a combination of human relationships and clear contractual terms. “You have to trust the people in the foxhole, from the Board to first responders,” said a subject matter expert.
- Amplify communications in a crisis. For example, a CISO said he was communicating with the Board hourly during the recovery efforts after a DDoS incident.
- Set realistic expectations for recovery. CISOs in the region reported that recovery from a DDoS attack can take weeks or months. Forensics alone often take 45 days or more. Ensure that senior management understands the time and effort realistically required to resolve different kinds of attacks.
- Establish a robust partnership strategy before an attack occurs. Engage other internal members of the crisis team, particularly Legal and Communications, and the Board of Directors, who will want to know that the CISO is being proactive and prepared for an attack.

An attorney recommended the following best practices:

- Update the response playbook. Include specific details about responding to a ransomware attack. Document incident identification and classification—the response playbook should detail how threats are evaluated and prioritized. Prepare a third-party communications plan in advance.
- Use the “cc” function broadly in e-mails. Avoid situations where someone can claim, “We didn’t know what to do when an incident occurs.” The CISO can’t go it alone. Communicate

and collaborate with Legal, Communications, senior management and external service providers so everyone is familiar with how to work together during an attack.

- Understand what you're paying to protect. Revenue, reputation, private personal information and other assets may be at risk.
- Be able to calculate whether restoration is more cost-effective than paying a ransom. The challenge of restoring data and vulnerable systems at speed and scale with SecOps systems resources stretched thin due to the current pandemic can drive the decision to accept ransomware demands.
- Reevaluate your ransomware payment policies. Four months ago, the attorney would never advise a client to acquiesce to a ransomware demand. The pandemic has made payment more common. Out of 100 cases prior to the COVID-19 disruption, only a few saw a ransom payment fulfilled. In today's operating environment, a quarter (4 out of 16) of ransoms have been paid in this attorney's case load.

Conclusion

Ransomware is clearly part of the APAC CISO's new reality. Successful CISOs are responding to the threat with a multi-faceted approach, addressing people, processes and technology to prepare for worst-case scenarios, such as a well-funded nation state attack. Adequate defenses and resilient recovery will take an up-to-date response playbook, transparent, trusted stakeholder relationships, robust technology tools and diligent monitoring.

CONTACT

Andy Vautier

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 509,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.