Ransomware: Addressing the rising threat

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "**Ransomware: Addressing the rising threat,**" on August 6, 2020. CISOs shared how they are responding to the threat of ransomware attacks, and discussed recent trends.

While ransomware attacks are not new, current operating environments make enterprises more susceptible to threats from nation-states and other cybercriminals who are approaching ransomware like a business. How should enterprises prepare for and respond to attacks? Is paying a wise business decision? Where are our greatest vulnerabilities?

Our subject-matter experts were Jacky Fox, Accenture Security managing director and security lead for Accenture Ireland; Mark Raeburn, Accenture Security managing director and global cyber investigation, forensics and response lead; and ACF members with significant experience in incident response. The session was hosted by Andy Vautier, Accenture CISO and ACF chair.

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.

Ransomware attacks increasing and evolving

Ransomware is evolving in new directions. Now, bad actors are not only taking control of a system and demanding a ransom, but also stealing data. A number of threat actor groups are publicly announcing what they have taken and are requiring a ransom for its return—with no guarantee that the exfiltrated data won't be sold despite a ransom payment.

In fact, bad actors are now behaving more like sophisticated businesses. They are demanding digital currency payments, which makes identification and attribution more difficult. Data is the most targeted asset. Cyber criminals are accessing enterprise privacy policies and other documentation, such as revenue and insurance deductibles, to calculate the perceived value of data and set their ransom demands accordingly. Criminals are investing in new capabilities and courting media coverage about their successes.

The World Economic Forum Centre for Cybersecurity Advisory Board 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 such as fileless attacks will most likely increase. The broader attack surface that arose out of the COVID-19 response (such as working from home and relying on insecure networks) makes ransomware attacks more attractive.

Payments on the rise

The challenge of quickly restoring data and vulnerable systems across the enterprise while security resources are stretched thin can drive the decision to accept ransom demands. Payment has become more common during the pandemic. Criminals are re-ransoming data by selling it to other bad actors, as well as reinvesting to make their attacks even more profitable. Paying a ransom doesn't always mean the data will be returned safely.

Timing is a critical factor in the decision to pay a ransom. Threat actors typically set deadlines of seven to 10 days, which may not be an adequate timeframe for mitigation or remediation. In cases where personally identifiable information (PII) is compromised, the opportunity to negotiate may be only 48 hours to five days.

A representative timeline outlines the process of a cybercriminal ransomware attack:

- Days 1-6: Establish a foothold; obtain elevated privileges to conduct lateral movement in order to identify sensitive data and critical assets, including back-ups.
- Days 7-13: Perform additional reconnaissance and exfiltration of data.
- Days 14-21: Conduct widespread or often highly targeted encryption designed to do maximum damage.
- Days 22 and beyond: Demonstrate successful compromise via display of data on a public website. Criminals are increasingly hosting their own sites for better control of stolen data. Demand a very large ransom as payment for a decryption key and the safe deletion of stolen data without leakage.

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. Perpetrators avoid detection by channeling ransomware proceeds via digital currencies that are cashed out outside the host country, and by never attacking victims inside the host country. This practice 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.

Prepare for the current reality

Several roundtable participants expressed concern that response playbooks are not keeping pace with an evolving threat landscape. 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, and exhibiting a business mindset to build capabilities and extract larger ransoms more frequently. In the extended environments in which enterprises are working during the COVID-19 disruption, the increase in endpoints poses its own unique challenges.

An ounce of prevention is worth a pound of cure. Conduct significant crisis planning and war-gaming around a ransomware attack. Pressure-test the arrangements and resources you have in place, the decisions you'll have to make, the thresholds you'll establish to pay or not pay in the context of your current operating environment. Consider establishing a "ransomware task force" to plan for and practice responses to ransomware demands. Set a high standard, such as countering the capabilities of sophisticated nation-states.

One possible preparation is to unleash a red team test without advance notification. Other suggestions include tabletop exercises that help the board and CEO of publicly traded companies prepare public statements about ransomware attacks that could impact financial markets.

CISOs need to develop strong partnerships to keep informed of ransomware developments and possible responses. Before an attack occurs, build relationships with:

- Other internal members of the crisis team, particularly legal and communications. The board of directors will want to know that the CISO is being proactive and is prepared for an attack.
- Law enforcement, which can be responsive and helpful. Engage the FBI and The National Counterintelligence and Security Center (NCSC). The U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) offers a variety of valuable information including ransomware alerts, best practices and training materials.
- Supply chain partners. Threat actors are testing third-party vulnerabilities as a means of attacking their ultimate targets. Assess and refine security breach notification policies to ensure that third parties keep you informed of attacks and their remediation obligations.

Best practices

1. **Get security right**—Focus on the basics. Keep your security hygiene up to standard; maintain controls and continue patching; ensure visibility into, and protection of, crown jewel data. Active Directory (AD) Domain Name System (DNS) protections, along with robust data back-up strategies, are routine but critical. And continue to emphasize security awareness training for all personnel.
2. **Be prepared**—Conduct ransom-based tabletop exercises; ensure you have an incident response plan for ransomware; prepare with senior executives, legal, the board, the security function and the media relations function; develop emergency communications; discuss the ethics of incident response with management.
3. **Monitor networks**—Increase network monitoring for data exfiltration; be alert for signs of an attack; look out for large movements of data. Monitoring penetration activity to detect threats is a key to preventing ransomware attacks. Some experts estimate that 80 percent of attacks occur on shadow IT networks or systems inherited during mergers and acquisitions.
4. **Protect endpoints**—Endpoint detection and response tools are a particularly important component of a layered approach to protect from ransomware attacks.
5. **Monitor ransomware news**—Attacks at other firms are a reliable indicator of future criminal activity. Bad actors often publicize their attacks, and successes will breed additional activity.
6. **Know your team**—The CISO can't do it alone. Collaborate and prepare with legal, communications, senior management and external service providers so that everyone is familiar with how to work together during an attack.
7. **Know your policies and procedures**—Your response playbook is the first thing regulators and litigants will ask for after a breach.
8. **Know your operations and options**—Can you quickly restore and back up data across the enterprise? Is your insurance coverage adequate? Are your security protocols protecting against data exfiltration?
9. **Know your contracts and partners**—Are your supply chain partners vulnerable to attacks, or are they working proactively to protect themselves and your enterprise? Ask partners about their coverage and what protections or remedies they can provide in the event of an attack. Meet with the appropriate law enforcement authorities before an attack to facilitate their support when an attack occurs.
10. **Consider cyber insurance**—Cyber insurance is a critical component of risk management. Policies are relatively inexpensive at the moment, but should be assessed carefully to ensure appropriate coverage. Evaluate policies carried by your enterprise and by important third parties.

Conclusion

Ransomware is clearly part of the CISO's new reality. We must continue to "up our game" to respond to the rapidly evolving ransomware landscape. Prepare as if attacks from nation-states are inevitable. Strengthen your defenses—in your people, processes and technologies—to inhibit threat actors who are behaving as if ransomware will be an increasingly profitable business. Adequate defense will take transparent stakeholder relationships, rigorous preparations, effective 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.