Ransomware reoriented

Why crisis management is at the heart of ransomware resilience

accenture

Business-led security

For many organizations, ransomware is seen as a technology or security problem—not an issue to be tackled by the business, for the business.

In a time of compressed transformation, organizations should adjust mindsets around the role of security following a ransomware event. Existing recovery strategies that are tuned to traditional business continuity plans are no longer enough. By understanding—and preparing for—the implications of ransomware across the whole organization, business leaders can recover more quickly when an attack happens. In short, a modern ransomware and extortion response should be treated as a business risk that prioritizes effective crisis management across the enterprise.

Key challenges

1. Traditional crisis response plans need to evolve—ransomware is a business risk, not simply a security problem.

2. Existing crisis communications plans lack the transparency and agility to adapt to new cyber complexities.

3. Ransomware is borderless—it impacts the enterprise, extended ecosystem and multiple stakeholders.

What are the challenges?

The ransomware evolution

In our State of Cybersecurity Resilience 2021 research, we found not only that attacks are on the rise, but also 20% of costs associated with all incidents were attributed to brand reputation damage. The recommendation? Get the balance right between security efforts and alignment with the business strategy.

In the immediate aftermath of a ransomware attack, it's vital to understand business priorities. Yet, it's often unclear who has decision-making authority or overall accountability, which can slow response and recovery efforts.

Defining a crisis decision framework up front involves identifying decision-making thresholds aligned to the business strategy, the organization's risk tolerance, its cyber communication strategy and clear accountability for both technical and business decisions during a crisis event. What's more, it's essential to regularly review that decision-making criteria, fine-tuning it over time to keep pace with organizational change.

From shaping the communication strategy, to implementing a balanced approach to threat containment and eradication—or tackling whether to pay or not to pay a ransom—documenting and exercising a crisis decision framework can help organizations better prepare, speed up responses and, ultimately, ease the pressures of extortion demands.

Response priorities

- What needs to be fixed first?
- What are the most important systems or data to restore?
- What does our organization's revenue rely on?
- What upstream dependencies exist across people, process, and technology components?

Let’s take a look at three key challenges that highlight the need for greater alignment between security and the business, before, during and after a cyber crisis event:

1

Traditional cyber incident response plans need to evolve—ransomware is a business risk, not simply a security problem.

Enterprise crisis response is a team sport and demands a business-focused crisis management function to deal with modern destructive events.

2

Existing crisis communications lack the transparency and agility to adapt to new cyber complexities.

A pre-defined decision framework, coupled with a greater understanding of the industry, its regulations, and customers, can support more robust crisis communications.

3

Ransomware is borderless—it impacts the enterprise, third-party ecosystems and multiple business stakeholders.

As attack surfaces evolve, crisis response needs to extend to address impacts on customers, corporate subsidiaries, suppliers, third parties, investment portfolios, and merger and acquisition targets.

Challenge

1

Traditional cyber incident response plans need to evolve —ransomware is a business risk, not a security problem

Recovery strategies in traditional business continuity and disaster recovery plans are no longer enough to deal with modern ransomware attacks.

Security teams' current approach to incident response typically involves solving the technical investigation aspects of an attack—how did the threat actor invade? Which systems were affected? What data was taken and from where?

But attacks are not simply a security problem. Incident response must also consider critical business processes and how they impact recovery priorities—how is the value chain affected? How much product do we have in stock? What's the impact on employees, customers and suppliers? What is our financial exposure?

Challenge 1

Key to successful ransomware recovery is standing up and stabilizing the most critical systems and operations first, then turning attention to the rest of the business. Failing to prioritize these business dependencies plays into the hands of attackers. For example, recent threat actor tactics include deleting or damaging backups so that they are unavailable—upending traditional business continuity or disaster recovery plans.

Prioritizing and stabilizing key operations and systems can help prevent additional downstream financial, reputational, operational and physical impacts.

Organizations should evolve traditional business continuity and incident response approaches. With greater collaboration, CISOs, COOs and other senior leaders can develop one cohesive plan that identifies the priorities for the whole business, problem-solve the big picture and better prepare for swift and inclusive business recovery.

By adopting a strong communications plan, leaders can tackle ransomware for what it is—a crisis that needs to be handled in a business-focused manner.

Challenge

2

Existing crisis communications lack the transparency to adapt to new cyber complexities

On any scale, ransomware incidents are disruptive and need an effective communications plan. But it's not a one-and-done event—regular updates shared with internal and external stakeholders are vital to get ahead of any unfolding story.

These communications should often not only balance speed with accuracy during a rapidly evolving event, but also be appropriate for different stakeholder audiences. Understanding the unique demands of an industry, its regulations and the notifications and disclosures that apply is fundamental.

Yet, many business leaders may be ill-prepared when it comes to communications. Although organizations may handle security incidents efficiently, unless they also communicate the status effectively, they may be subject to a public business disinformation campaign or risk erosion of confidence in the business—or lose customer trust.

Challenge 2

Every communications plan is nuanced depending on reporting obligations. And industries need customized strategies—for instance, stolen healthcare data involves notifying patients, whereas a bank may need to prioritize the stringent requirements of leading financial regulators around the world.

As organizations strive for digital trust with customers while people become more aware of privacy concerns, it becomes even more important to be open and honest about what has happened and what happens next—internally and externally.

Applying a traditional corporate communications response in isolation from the rest of the business will not be enough. Collaboration with security professionals, legal teams and the organization's broader ecosystem makes sure communications teams have a structured approach and that they act with transparency, in a thoughtful and factual way.

Key questions

- ☑ What happened?
- ☑ What do we know?
- ☑ Who was impacted and how?
- ☑ When did it happen?
- ☑ What are we doing about it?
- ☑ What's next?

Our agile approach to cyber crisis communications

Accenture has developed the following ransomware response and recovery approach to handling cyber crisis communications:

1. Triage and prepare

Identify impacted parties and align on reporting objectives, tone, timing, audience and notification requirements.

2. Develop and approve

Develop messaging aligned to the communications strategy, identify mediums for each stakeholder group and obtain approvals.

3. Posture and deploy

Reinforce messaging, train employees, setup monitoring and deploy a vertically integrated communications taskforce.

4. Monitor and evaluate

Employ an agile approach to evaluating and iterating through updates based on defined metrics, sentiment analysis, media outreach, financial and brand impact.

Challenge

3

Ransomware is borderless—it impacts the enterprise, third-party ecosystems and multiple stakeholders

Too often, ransomware destruction extends beyond the encryption of data—systems are down, customers cannot be contacted and the business is disrupted.

Indeed, as a result of the impact on organizations' critical infrastructure in 2021, law enforcement and government became even more involved with ransomware threat actors. For example, the Office of Foreign Assets Control (OFAC), a financial intelligence and enforcement agency of the United States Treasury Department issued new guidance in September 2021 warning companies that to pay or facilitate payment of a ransom to a sanctioned entity will be subject to civil penalties.[1] For the first time, the Treasury Department recently sanctioned a Russian-owned virtual currency exchange.[2] These and other actions by federal agencies have put threat actors under pressure to find new ways to be profitable.

As a result, threat actors evolved their tactics. In some cases, they focused less on encryption and destruction and more on stealing data and then extorting a victim by threatening to disclose stolen data. This approach delivers quick impact and makes attribution more difficult.

Challenge 3

Today, you can buy access and malware and simply execute a ransomware attack by becoming an "affiliate" of a ransomware-as-a-service (RaaS) program available on criminal forums. An affiliate only needs to provide proof of their technical skills to ransomware groups to start distributing ransomware and receiving payments. Compounding this challenge, compressed transformation has often extended the attack surface—evidenced by the triple-digit increase in attacks observed in 2021.[3]

Despite heightened awareness, government action and industry collaboration, ransomware is without borders and remains a persistent threat. Any crisis response strategy should take into account the range of stakeholders affected—customers, corporate subsidiaries, suppliers, trusted third parties, financial investments and merger and acquisition targets. Conversely, the response strategy should also address how to respond when any one of these stakeholders is attacked. For example, many businesses rely on a third-party payroll service. What is the appropriate response when a key stakeholder entity is impacted?

107% increase YoY in ransomware and extortion attacks

33% of intrusion volume from ransomware and extortion

Top five countries: 47% of ransomware attacks impacted organizations based in the US, followed by Italy (8%), Australia (8%), Brazil (6%) and Germany (6%).

Source: Accenture Cyber Investigations, Forensics & Incident Response Engagements

Back to business

Despite implementing encryption techniques in all the right places, a leading manufacturing company experienced a devastating ransomware attack. The company faced a dramatic crisis—it could not produce, ship or sell any of its products. Its supply chains were compromised. Employees were unable to log into their laptops. No one could answer calls from customers in the call centers. And critical files, such as the details needed for a financial close in four weeks' time, were inaccessible. Making matters worse, the CEO was informed that two back-up locations were also affected.

We worked closely alongside the client's executives to address the impact of the attack by:

- Managing vital technology aspects—cleansing systems, providing reasonable assurance that the hacker was no longer present and rebuilding systems in the right order.
- Focusing the manufacturer's executive committee—establishing a deep connection between the cybersecurity team and the enterprise business strategy.
- Executing an effective communications plan—targeting employee, client and partner stakeholder audiences.
- Employing a first-of-its-kind playbook —clearly identifying the business areas where actions needed to be prioritized.

The team restored the most critical business systems—manufacturing, distribution and customer facing call centers—within the first week. Remaining business operations were restored and all factories were back online in just four weeks.

Modernizing ransomware response

Here are some practical steps to help manage and modernize a ransomware response:

Step 1

Enhance your business preparedness

Understand your value chain across every area of the business and what your priorities are in the event of an attack. Organizations should know with confidence and uniformity the many moving parts that make them profitable.

Critical business processes, their underpinnings, and downstream dependencies are often poorly understood or overlooked in a typical incident response plan.

For example: Shipping products may depend on a distribution center's label printer, so making that operational, rather than fixing some of the larger systems or devices, might be the quickest way to minimize disruption.

Step 2

Communicate openly with care

Define a communications strategy that is agile and considers the complexities of a cyber event, from a technical and business perspective.

Organizations should be cautious to avoid sharing incorrect information and this is often industry-dependent, so it's vital to assess all the facts, set the tone and be thoughtful before the communication process begins in earnest.

For example: In financial services, stolen credit card information will be subject to stringent regulatory and compliance demands before the general public should be made aware of the breach.

Step 3

Get the CEO and board—on board

Testing and validating attack prevention, detection, response and recovery is a way of life for most organizations, but this practical step can be enhanced by drawing on the CEO and Board.

Tabletop exercises are generally undertaken by security personnel. By evolving such exercises to include executive-level simulations, organizations can not only test their defenses against a typical ransomware attack, but also introduce the risk and adrenalin of a “real life” attack scenario.

For example: Executives may be told there are three lines of business down due to an attack where a threat actor is asking for US$10M. Executives are asked to determine in real time which business should be recovered, how they communicate their response and who is responsible for making those decisions.

Are you ready?

The evolution of ransomware and extortion events requires a different way of thinking—one that is business and security focused.

Ask yourself:

- Are our business executives aligned with security teams to handle new ransomware crises?
- Do we have the right communications plans in place to roll out an effective response?
- Have we established the risk-based decision factors associated with an outage?
- What actions can we take and processes can we put in place today that can help us to recover more quickly?
- What is our financial threshold if we cannot ship products?
- How much product do we need in reserve if we can't manufacture for three days?

With more agile, robust and transparent crisis management capabilities, organizations can handle ransomware events better and improve overall cyber resilience.

Authors

Robert Boyce
Managing Director,
Accenture Security
Global Incident Response
& Transformation Lead

Ryan Leininger
Senior Manager,
Accenture Security
Global Proactive &
Readiness Services Lead

References

1. Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, U.S. Department of Treasury
2. Treasury Takes Robust Actions to Counter Ransomware, U.S. Department of the Treasury
3. Accenture Cyber Investigations, Forensics & Incident Response Engagements conducted between January and December 2021.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services—all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. 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 @AccentureSecure on Twitter or visit us at **www.accenture.com/security**

This document refers to marks owned by third parties. All such third-party marks are the property of their respective owners. No sponsorship, endorsement or approval of this content by the owners of such marks is intended, expressed or implied.

This content is provided for general information purposes and is not intended to be used in place of consultation with our professional advisors.

Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. The information in this report is general in nature and does not take into account the specific needs of your IT ecosystem and network, which may vary and require unique action. As such, Accenture provides the information and content on an "as-is" basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report. The reader is responsible for determining whether or not to follow any of the suggestions, recommendations or potential mitigations set out in this report, entirely at their own discretion.

220023