Forrester's Guide To Paying Ransomware

Paying Ransom Can Be A Valid Recovery Option Based On Business Need And Circumstances

by Josh Zelonis and Trevor Lyness
with Stephanie Balaouras, Madeline Cyr, and Peggy Dostie
June 5, 2019

Why Read This Report

Conventional wisdom says that when your company suffers a ransomware attack, you should never pay the ransom. But hardline conversations about whether to negotiate with cybercriminals takes a backseat to the reality that we're all beholden to the business and its key stakeholders. This report helps security pros understand the process of responding to a ransomware incident and deciding if paying a ransom is sometimes the best business decision.

Key Takeaways

A Ransomware Attack Is A Data Breach
Unauthorized code execution by a third party that accesses and encrypts business-critical data is a data breach. Don't just settle for decryption; investigate to understand if there has been exfiltration, and be sure to remove the unauthorized access to your infrastructure.

Attackers Are Targeting Your Recovery Capabilities
Ransomware attacks are up 500% from this time last year, and more organizations than ever are finding themselves having to pay the ransom as attackers become more sophisticated and specifically go after your backups.

Paying A Ransom Is A Business Decision
Although companies should generally seek to avoid paying a ransom, it's a valid recovery path and should be explored in parallel with other recovery efforts to ensure you're making the best decision for your organization.

Forrester's Guide To Paying Ransomware

Paying Ransom Can Be A Valid Recovery Option Based On Business Need And Circumstances

by Josh Zelonis and Trevor Lyness
with Stephanie Balaouras, Madeline Cyr, and Peggy Dostie

June 5, 2019

Table Of Contents

2 **Ransomware Is A Persistent Threat To Your Business**

Companies Are Increasingly Opting To Pay The Ransom

3 **Make The Right Business Decision For Your Organization**

Assemble Your Cyberincident Response Team

Bring In A Ransomware Expert

Recommendations

7 **Follow Five Best Practices To Plan For Ransomware Attacks**

8 **Supplemental Material**

Related Research Documents

The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2019

Ransomware Is A Business Continuity Issue

Ransomware Protection: Five Best Practices

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Ransomware Is A Persistent Threat To Your Business

The number of ransomware attacks on enterprises is up 500% from this time last year, and these attacks are projected to cost businesses $11.5 billion in 2019.[1] Threat actors are becoming increasingly sophisticated in how they ply their trade: identifying the critical assets to interfere with core business functions, seeking out and specifically targeting your backup systems to undermine your ability to recover, and, in some cases, researching your company's financial situation to know exactly how the attack is affecting it and how much you can afford to pay. Ransomware is a business, and these actors want to get paid.

Companies Are Increasingly Opting To Pay The Ransom

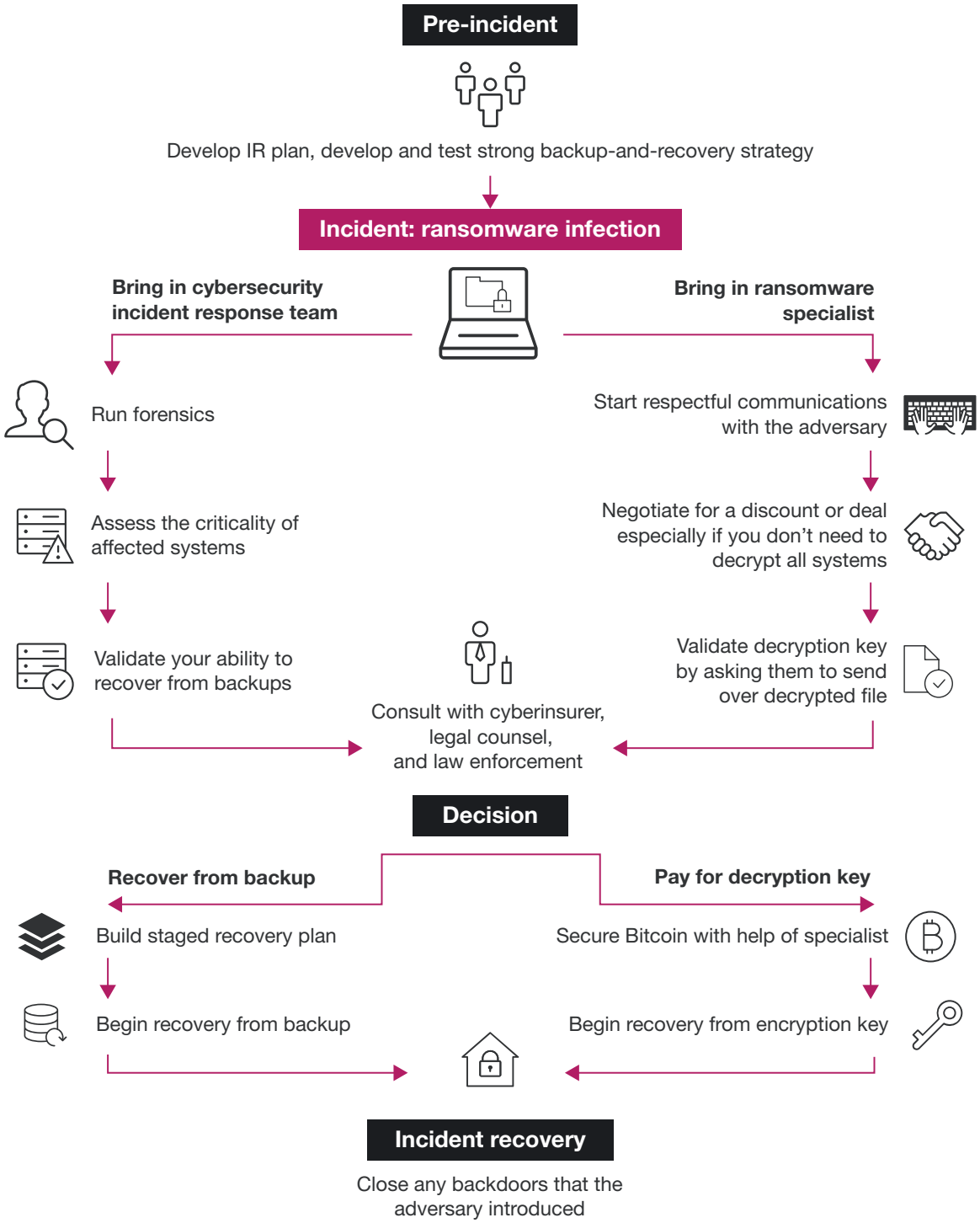
The conventional recommendation is to never pay a ransom. However, security professionals are beholden to the business' financial interests and its key stakeholders — which may mean going against conventional wisdom. Forrester has been tracking a notable increase in ransomware payouts. After examining several of these cases, we now recommend that even if you don't end up paying the ransom, you should at least consider it as a viable option. Here are a few thoughts to consider if you find yourself in this unenviable situation:

- **In some circumstances, paying the ransom may be the best option . . .** Loss of core business function can be catastrophic to your organization. As ransomware grinds on, daily business operations come to a halt, and you may find your organization scrambling to find new ways to meet core functions, which puts stress on everyone. This problem is complicated even if you have good backups that survived the attack. Many organizations significantly underestimate the scale of disruption they need to plan for or make too many assumptions about what functionality will continue to exist after an attack.
- **. . . but paying a ransom doesn't magically solve your problems.** When paying a ransom, there are always questions about whether decryption keys exist, if the extortionist will deliver those keys to you, and even how your organization is going to scale decryption efforts across your infrastructure. While there may be a thieves' code that double-crossing victims is bad for business, if extortion was not the motivation behind the attack, you may never see decryption keys. Even in a best-case scenario, decryption at scale often requires a cadre of consultants and introduces problems such as available disk space and wonky decryption code. Further, to avoid becoming a repeat customer, it's important to address any persistence an adversary may have introduced into your environment.

Make The Right Business Decision For Your Organization

The average ransomware incident lasts 7.3 days, but this may vary from several days to weeks or even months depending on the scale of the attack and the strain of ransomware.[2] Whether you're decrypting systems, restoring from backups, or starting over from scratch, recovery requires significant staffing and time. Once the attackers have encrypted your environment, your organization needs to start the two parallel processes of initiating a conventional cybersecurity incident response and establishing communication with the adversary. Performing these processes in parallel will help inform the decisions of the business and speed recovery (see Figure 1).

FIGURE 1 Ransomware Incident Response Workflow



Assemble Your Cyberincident Response Team

Ransomware recovery is a massive group effort. This is not an endeavor that should be undertaken without careful planning, so be sure to include ransomware as a contingency in your business continuity planning, as well as your cybersecurity incident response planning. You need to immediately notify and gather your cyberincident response team and start down the road of the recovery process:[3]

- **Engage your incident response provider immediately.** In a ransomware attack, you've been breached; an adversary has accessed devices on your network and demonstrated the ability to perform unauthorized code execution. You need to verify if attackers have exfiltrated any customer data and engage your legal team to assess relevant breach notification laws. Your response will require your incident response provider to run forensics to ensure the attacker is fully purged from your network.
- **Assess the criticality of all affected systems and build a staged recovery plan.** Your immediate recovery objective is to restore business-critical functionality. Focus on systems that affect your ability to do business with your customers and sensitive data at risk of permanent loss. The output of this process will help you recover faster, regardless of the method of recovery you eventually undertake.
- **Validate your ability to recover from backups and build a timeline for doing so.** Identify the extent to which your company can restore from backups and what that recovery point will be. Once you've established the ability to restore from backups, build a realistic timeline based on the scale of the attack. Many organizations drastically underestimate the time it takes to do this because they test recovery infrastructure on systems in isolation, not at the scale of a major attack.
- **Engage with external stakeholders before you make any decision.** If you perform certain actions before notifying your cyberinsurer of the breach, the insurer may not fully cover your response. Even if you don't think you have cyberinsurance, check with your broker to see if you have coverage under other insurance policies such as property and casualty, professional liability, crime, or kidnap and ransom.[4]

Bring In A Ransomware Expert

Ransomware negotiation specialists regularly help organizations recover from ransomware attacks and can help identify the business case for paying (see Figure 2). They bring not only a wealth of knowledge about specific types of ransomware, but they potentially even have experience with the specific actor you're dealing with. Forrester has identified six companies that specialize in this capability: Coveware, Cylance, Cytelligence, Flashpoint, Kivu Consulting, and NEST Consulting. As you work with these specialists:

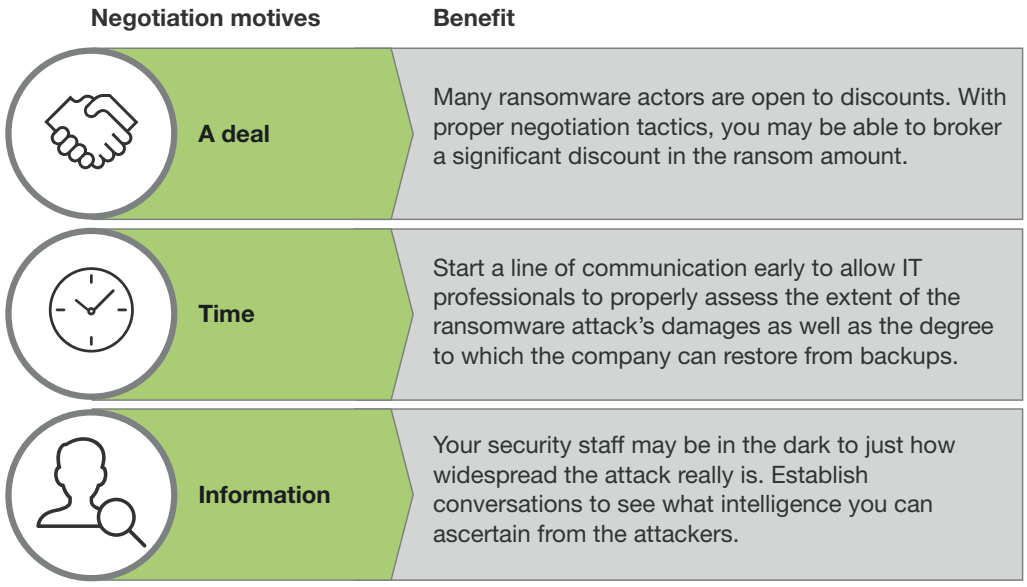
- **Determine your recovery timeline and likelihood of success using decryption.** Ransomware negotiation specialists will help you procure proof of life to hedge risks and ensure that the attackers can deliver upon ransom payment. These specialists are often familiar with specific ransomware actors and, knowing the actor's past history, can help you understand the likelihood

of success. They'll also use their knowledge of the specific ransomware strain to help you build a decryption timeline. For instance, a large server may take only minutes to decrypt when dealing with LockerGoga, but as long as a full week for Ryuk.

› **Be polite when engaging attackers.** Nothing good comes from acting disrespectful to people, but the stress and frustration of suffering a ransomware attack has caused more than a few to lose their cool. You may not like it, but you very well may need something from these attackers: This is a business transaction. Another good reason for using a specialized ransomware negotiator, even beyond their specific expertise, is that they're emotionally disconnected from the attack, which lets them maintain a necessary level of professional decorum when interacting with these attackers. Keep in mind, ransomware actors are also operating at scale; you're most likely not their only client, and they don't need you to survive.

› **Consider paying for only a few critical systems.** In scenarios where you have backups or can feasibly recover systems from ransomware with enough time, you may opt to pay the ransom for only your most critical systems. Sophisticated ransomware actors may have enough knowledge to understand they can charge you more for critical systems, but by paying for only a fraction of your encrypted systems, you may still get a significant discount. This is another time when the output from the parallel process of building out a staged recovery plan becomes important.

FIGURE 2 Three Strategies When Negotiating With Ransomware Threat Actors



Recommendations

Follow Five Best Practices To Plan For Ransomware Attacks

Documenting your ransomware response ahead of time is the best way to ensure you'll be prepared to react when ransomware hits. Here are five best practices security professionals should follow to prepare their ransomware response:

1. **Invest in cyberinsurance or business interruption insurance.** Large-scale ransomware attacks and seven-figure ransom demands are becoming more and more common. Insurance lets you transfer your financial loss risk directly to your insurer. However, be aware that it's becoming more and more common for cyberinsurers to invoke the "acts of war" clause to avoid compensating clients for their losses. When shopping for cyberinsurance, research what payments an insurer has paid or not paid as part of your due diligence before considering yourself covered.
2. **Benchmark your ability to recover from backups at scale.** A harsh reality is that a majority of organizations aren't testing their ability to recover a single system from backups, much less validating they have the ability to recover potentially hundreds of systems at the same time.[5] Include ransomware in your business continuity planning, and don't take for granted that you can recover from backups. Only by testing your ability to restore at scale beforehand can you support the recovery-time estimates on which your organization bases business decisions regarding ransom payments. You should have a documented BC and IT DR plans specific to ransomware attacks. Generic, impact-based plans (e.g., loss of IT, loss of facilities, loss of people etc.) won't suffice.
3. **Have a plan for acquisition and payment of cryptocurrency.** Volatility in the cryptocurrency markets complicate any recommendation for buying and holding cryptocurrency for the purpose of paying ransoms. Finding the funds to pay a five-, six-, or seven-figure ransom at a moment's notice can be particularly tricky for companies that don't have spare cash floating around. This may be something a ransomware specialist can facilitate, but don't find yourself needing to buy seven figures' worth of Bitcoin without a plan.
4. **Enter into a retainer agreement with a cybersecurity incident response provider.** Whether you're a large enterprise or medium-size business, given today's evolving threat landscape, everyone is a target. A preexisting retainer is like having a fire extinguisher in your house: It pays to be prepared if there's a fire.[6]
5. **Identify a ransomware expert whose goals align with your own.** The explosion of ransomware attacks is quickly making ransomware negotiation expertise a best practice. However, it's a fledgling market performing a service that makes some people uncomfortable. Until the market stabilizes and develops a set of established best practices, the best criterion for selecting a vendor is a shared mission. Your organization is going to be putting a lot of faith into this firm; finding a vendor before the incident whose goals align with your own will limit anyone second-guessing your own decisions later.

Supplemental Material

Companies Interviewed For This Report

We would like to thank the individuals from the following companies who generously gave their time during the research for this report.

Aon
Cisco
Coveware
Cylance
Cytelligence
Flashpoint
NEST Consulting

Endnotes

[1] Source: "Cybercrime tactics and techniques Q1 2019," Malwarebytes (https://resources.malwarebytes.com/files/2019/04/MWB-CTNT-2019-state-of-malware_FINAL.pdf) and Steve Morgan, "Global Ransomware Damage Costs Predicted To Hit $11.5 Billion By 2019," Cybersecurity Ventures, November 14, 2017 (https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/).

[2] Source: "Ransom amounts rise 90% in Q1 as Ryuk increases," Coveware blog, April 16, 2019 (https://www.coveware.com/blog/2019/4/15/ransom-amounts-rise-90-in-q1-as-ryuk-ransomware-increases).

[3] See the Forrester report "Planning For Failure: How To Survive A Breach."

[4] See the Forrester report "Your Guide To Cyberinsurance."

[5] See the Forrester report "Ransomware Is A Business Continuity Issue."

[6] See the Forrester report "The Forrester Wave™: Cybersecurity Incident Response Services, Q1 2019."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.