arcserve®

A Ransomware Crisis Plan is Now a Business Imperative

Create yours and you'll be empowered to circumvent cyber criminals and protect your reputation

The Digital Era has ushered in a period of massive disruption, enabled by connection and access to information like we've never seen before.

Unfortunately, organized crime is no exception. Cyber criminals around the world have seized upon their digital opportunity and built a burgeoning $5 billion extortion racket—and they show no signs of closing-up shop.

This isn't a surprise to those of you in IT, of course. Ransomware attacks are now part of your daily news diet. What's more, data security and backup and recovery vendors are regularly beating the ransomware drum. Everywhere you turn, you're bombarded by the threat—and you may very well be experiencing some ransomware fatigue.

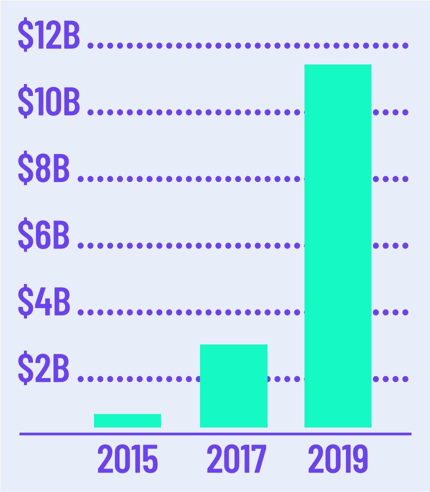
Still, you must be cognizant of the fact that ransomware represents an existential threat to your organization—and prepare accordingly.

Attacks today often extend beyond a few workstations; whole systems can be shut down, not only denying access to critical applications and files, but knocking out phones, email, and Internet, as well. This could mean significant—even unrecoverable— financial and reputational losses. Arcserve research shows that consumers have little tolerance for ransomware-related disruptions - 59% of consumers would likely avoid doing business with an organization that had experienced a cyberattack in the past year. Additionally, 70% of consumers believe businesses aren't doing enough to adequately secure their personal information and assume it has been compromised without them knowing it. Big or small, public or private—today, no organization is immune.

This is precisely why you need to create and maintain a ransomware crisis plan. Armed with this documentation, you'll be equipped to mitigate the negative consequences of a ransomware attack, ensure rapid restoration of your business operations, and protect your brand.

Ransomware is on the rise

Ransomware campaigns have proven to be a profitable enterprise for cyber extortionists, netting a predicted $20 billion in 2021, according to cyber security research firm, Cybersecurity Ventures. This represents a whopping 57X increase over 2015. Furthermore, Cybersecurity Ventures concludes that ransomware attacks occur with stunning frequency today. In fact, an attack is executed every 14 seconds and projected to increase to an attack every 11 seconds by 2021.



Ransomware-as-a-Service, or RaaS, is a primary driver of this upward trend—and it suggests a frightening new reality for IT professionals and corporate executives, alike.

That's because anyone can now get into the game, regardless of their technical chops. We're talking professional con artists who've successfully operated traditional social engineering scams—now enabled to apply their skills to ransomware without ever having to setup infrastructure or program a backend system.

It's a frightening reality of the Dark Web

Those with criminal intentions can now acquire RaaS for free or a nominal fee, and simply share a cut of the profits with their software provider. As a result, we expect the growing number of attacks to employ more creative approaches, as well.

Create your rock-solid ransomware crisis plan

Your ransomware crisis plan is mission-critical to the continued operations of your entire organization—which is why it simply can't be created in isolation. It requires the input of not only IT professionals, but critical stakeholders within each department to ensure you accurately assess business risk and mitigate impact.

Not sure where to start?

Let us walk you through the essential components of your plan.

1. Establish your ransomware crisis team

In the event of a crippling ransomware attack, your response won't be entirely technical. Therefore, your ransomware crisis plan can't be, either.

Consider the devastating consequences of some attacks—people are losing their jobs and companies are going under. It's imperative that you have executive-level involvement to ensure the ransomware crisis plan you develop sufficiently mitigates business risk and defines both your technical and communications response. What's more, you may need to make difficult financial decisions and address compliance issues in the face of an attack.

With this broad and deep team, you'll swiftly make informed decisions about which data, applications, and systems can be down or lost, and which represent a business sustainability threat— enabling you to proactively implement the solutions necessary to protect what you've deemed as mission-critical. Likewise, you'll communicate from a position of strength and convey a sense of confidence to both your internal and external audiences.

For financial, healthcare, and other organizations that adhere to strict compliance and data privacy laws, we also suggest you include your corporate counsel to ensure you reduce your legal liability to the extent possible.

Even if your organization isn't required to comply with data compliance and privacy requirements, we recommend a legal review of your final ransomware crisis plan to ensure you've dotted your I's and crossed your T's. You'll also want direction regarding the scenarios which should trigger attorney involvement—when customer data is hacked, for example.

Now that you have identified the key members of your team, be sure to document their contact information—including after-hours contacts. You'll also want to identify where the crisis team will meet in the event of emergency, so you can execute on your plan as efficiently as possible.

As such, your crisis team should include the following key voices:

- C-suite Leadership
- Director of IT
- Director of Comm's
- Department Chiefs
- PR Leadership
- Regional Sales Leadership

2. Document your governance plan

It’s not enough to identify your team. You must also define roles and responsibilities for each crisis team member to ensure a clear chain of command and efficient response when tensions are heightened.

✓ Technical Response

When it comes to your technical response, we recommend your CSO or director of IT take the lead. They’ll best understand the repercussions of each decision on a technical level.

✓ Communications Response

As for your communications response, you’ll need to identify:

1. Who drafts your communications
2. Who will be quoted
3. Who will sign off on all communications
4. If you’re allowing interviews, who will respond

✓ Ransom Response

With a properly designed disaster recovery strategy in place, you can recover and deny cyber attackers their payday.

If an attack threatens the sustainability of your organization, considering a ransom payment should be a last resort. Keep in mind that paying a ransom doesn’t guarantee data recovery – a SentinelOne report found that only 26% of organizations that made ransom payments were able to unlock their files.

If you make the risky decision to pay the ransom, you’ll need to identify both who will approve the payment and who will release the money; this is often your CFO. Remember to clearly identify and communicate the risks of not recovering data even if the payment is made.

When each of these decisions have been made, they should be documented in your ransomware crisis plan with absolute clarity—and everyone on your team should review and sign-off on their roles, responsibilities, and clear understanding of the risks involved.

3. Determine if you are ready to take the risk of paying the ransom - and if so, how

If caught without a robust disaster recovery strategy in place, organizations put themselves at risk of not having the processes in place to properly respond to cyberattacks. The immediate effects of an attack regarding data loss and downtime can cripple your organization, but long-term consequences can be far-reaching, including lost jobs and revenue, and loss of consumer trust.

FBI guidance states that organizations should never pay the ransom—and that stance makes sense from a law enforcement perspective. From a business perspective, when faced with the inability to function, executives will evaluate all options to protect their shareholders, employees, and customers.

According to its Ransomware Prevention and Response to CISOs document, the FBI recommends ransomware victims consider the following factors:

- Paying a ransom does not guarantee an organization will regain access to their data
- Some victims who paid the demand were targeted again by cyber actors
- After paying the originally demanded ransom, some victims were asked to pay more to get the promised decryption key
- Paying could inadvertently encourage this criminal business model

To avoid having to pay a ransom, map out your systems, data, and applications, documenting the following for each:

- Downtime costs
- Data loss costs
- Availability requirements

This information will provide the insight you need to build your disaster recovery SLAs as part of your disaster recovery plan – without it, you will be put in the position to consider paying a ransom.

We urge you to engage in this discussion now, while cooler heads prevail, and document your decisions clearly.

If your organization, as a last resort, would decide to take the risk and pay the ransom, you'll need to prepare the process of how you'll pay it. In most cases, cyber extortionists will demand payment in untraceable Bitcoin.

What you might not realize is there's a process for setting up an account, which might take four to five days before you can purchase Bitcoins. If you've been given a 72-hour window to pay the ransom demand, you may not make it in time.

To prepare for the risky move of paying, you could consider setting up an emergency ransomware fund, or establish a Bitcoin retainer—contracting with an organization that has Bitcoins in the bank already or the ability to get them quickly—so you can purchase them when needed. Do your research now and commit your process to the ransomware crisis plan – but remember, paying ransom does not guarantee recovery of the data.

4. Purchase your cyber insurance policy

The cost of a data breach or loss is so significant today, we suggest every organization seriously consider purchasing a cyber insurance policy.

In the event of a security breach, your cyber insurance policy may cover:

- Value of the data loss
- Data loss fees and fines
- Printing and postage costs associated with registered mail notifications

Of course, you'll need to thoroughly evaluate potential cyber insurance providers to ensure you've adequately protected your organization. Be sure to ask:

- How must I report an incident?
- What is the reporting window to get my claim covered?
- How do I ensure our coverage remains intact if we update our IT security environment?
- What first-party damages does this policy cover?
- What third-party damages does this policy cover?
- Does this policy cover cyber extortion?
- Does this policy cover the cost of regulatory fines and penalties that might arise from a ransomware attack?
- Does this policy cover retroactive intrusions or infections we may not have discovered yet?
- Does this policy cover infections introduced by personal devices and used for business purposes (BYOD)?

When your cyber insurance policy is in place, we encourage you to document your coverage within your ransomware crisis plan—as well as the contact information for your insurer.

5. Define the steps end users should take upon discovering an infection

According to Digital Guardian, spear phishing is responsible for 91% of all hacks today. So, it makes sense to consider your end users within the scope of your ransomware crisis planning.

What actions should your employees take if they become infected? And, who should they contact?

Within the four walls of your IT department, the answers to these questions might seem obvious. They may not be quite so clear to your less tech-savvy end users, however.

So, document those steps, which most likely include:

- Shutting down the computer
- Disconnecting the machine from networks and external drives
- Immediately contacting IT

Then, reinforce the importance of your end user protocol during your regular employee cyber security trainings.

6. Thoroughly document your technical response

In the event of a ransomware infection, a well-documented technical response will give your entire team greater confidence in their work and enable them to mitigate the negative impacts to your organization.

What should you consider as you develop your technical response checklist?

Your most immediate action will involve isolating any infected systems. If you can, disconnect from the Internet and your WAN connection to contain the ransomware.

Of course, not all organizations have the luxury of flipping a switch and going offline. If you host your own web servers and receive customer orders through your website, for example, you won't be able to fully disconnect without suffering some potentially significant consequences.

In collaboration with your crisis team, determine your path forward:

- What can be immediately disconnected from your network under any circumstance?
- What systems have little tolerance for downtime?
- Of those critical systems, under what circumstances should they be disconnected?

You'll also need to have a thorough understanding of your infrastructure, including network shares, local hard drives, and system interdependencies, so that when you do restore, you're able to reconnect everything—and in the right order.

Next, you'll need to diagnose the scope of your ransomware infection.

Starting with your first infected machine, we recommend you identify its access to the following:

- Mapped or shared drivers
- Mapped or shared folders from other computers
- Network storage devices
- External hard drives
- USB storage devices
- Cloud-based storage

Then, determine if any of these components of your file infrastructure are likewise encrypted or compromised.

Alternately, you can review the ransomware-generated registry or file listing to identify which files were encrypted.

Now, it's important to not only understand how far the ransomware has spread, but to identify the strain of ransomware that has infected your systems, as well. This insight may inform how you move forward. Keep in mind that there are strains of ransomware out there from which you simply can't recover. In those cases, it's best to know before you put a lot of labor and financial resources into an impossible data recovery. In other cases, IT security companies have built decryption tools which will enable you to circumvent attacker demands.

What if it's a new strain of ransomware?

A number of endpoint protection and antivirus vendors, as well as security research groups may be in a position to help. Upload a file or two, and they'll help determine the strain, so you can chart your best course of action.

Finally, establish your disaster recovery plan.

With a thorough map of your infrastructure and insight from key stakeholders on the criticality of your data, applications, and systems, document the level of availability required for each—and put high availability and disaster recovery solutions in place that enable you to deliver against your RPO and RTO requirements.

Furthermore, ensure you're executing regular and redundant backups. We highly recommend you adopt a 3-2-1 backup strategy:

To further enhance your ransomware crisis plan and address the growing trend of cyberattacks on backup data, consider incorporating integrated cyber and data protection as part of your proactive approach to ransomware. Assess solutions with anti-ransomware technologies or those that combine system and data protection to protect backups from cyberattacks and data loss.

With this information at the ready—and well-documented within your ransomware crisis plan—your crisis team will be empowered to determine the best course of action:

- Restoring from a recent backup—
  your unquestioned best path forward
- Leveraging a third-party decryptor to recover data
- Consigning yourself to the data loss
- Negotiating with attackers and paying the ransom

3. Maintain three copies of your data

2. Two of your copies may be local, but one must be offline

1. One copy must be off-site

7. Plot out your detailed communications response

In the event of a ransomware attack, what you say—and how you say it—will be just as important as what you do. Your response to this event will shape perceptions of your reputation inside and outside the organization, after all.

That's why having a well-defined communications plan in place before a crisis erupts is so important. It will empower you to respond with more immediacy and project confidence and control.

Where do you begin?

1. Document audiences that will require immediate notification, including:

- Customers
- Employees
- Attorneys
- Other major stakeholders

2. Identify who will communicate your messages—and how:

- Who will handle press inquiries?
- Who will be your spokesperson and, if you're a global organization, who will be your spokespeople within each region?
- Will you post anything directly to your website?
- How will you tell your customers and partners—by email only or by email with a calling campaign to your top contacts?
- How will you communicate with your key audiences if your primary means of communication are temporarily knocked out?

These are the kinds of decisions you'll want to make with your ransomware crisis team before you're ever faced with a crisis event.

3. Create canned crisis responses for each of your primary audiences—and for each of your communication platforms, including email, website, phone, and social media

While there will be variances determined by the specific ransomware strain and the magnitude of the infection, initial response, status message, and resolution message templates will enable you to communicate quickly and clearly, despite rising pressure.

4. Create communications best practices documentation for your customer-facing teams in advance, keeping in mind that their communications should be not only brand-aligned, but authentic, as well

There's nothing quite like a sweeping Twitter firestorm, fueled by copy/paste corporate responses, to remind you of the value of authenticity. In doing so, you'll align your entire organization to your corporate strategy and ensure an employee doesn't inadvertently say the wrong thing in the wrong way and create a reputation crisis or open you up to greater liability.

5. Develop an internal communications plan that will enable you to swiftly share information with your employees

- The nature of the ransomware attack
- How the infection will temporarily impact business operations
- Regular recovery status updates

No matter how you choose to disseminate your internal communications, whether it's an email from the CEO or a company call, you'll face a degree of frustration on the part of your employees; they may be unable to do their jobs or required to operate offline, adding inefficiencies to their processes. In short, they'll feel helpless.

Develop an internal communications plan that validates their frustration and keeps them in the loop. By providing regular updates—daily statuses at a minimum—you'll give them visibility into the progress being made and help minimize the impact on company morale.

8. Protect and practice your plan

Protect the integrity of your ransomware crisis plan

Your well-developed ransomware crisis plan can help you successfully navigate the rough waters that will invariably follow an attack—but only if you can access it when you need it most.

That's why we recommend you maintain digital copies of your plan onsite, offline, and in the cloud. What's more, we suggest you keep multiple hard copies of your plan, as well.

You must also keep in mind that your crisis plan can only be effective if it's kept current. So, regularly review it— at least once or twice a year—and update your documentation to reflect any changes to your ransomware crisis team, IT infrastructure, and communications templates.

In doing so, you'll ensure your plan is the effective tool it's designed to be when a ransomware attack hits. And, let's face it—today, it's not a matter of if, but when.

Practice your response to a ransomware crisis

Your ransomware crisis plan is a critical component of your recovery, but you'd be remiss if you didn't also consider the human component. With so much on the line, emotions will be heightened during an attack. If you regularly practice your ransomware response, however, your team will run like a well-oiled machine when faced with a real scenario.

Whether monthly or quarterly, engage your IT team in a disaster recovery exercise to ensure:

- You've confirmed SLAs
- You've identified and resolved vulnerabilities
- Your team has had the opportunity to encounter challenges and learn from them—before disaster strikes

Likewise, engage your customer-facing teams in at least bi-annual communication discussions and exercises to ensure they feel empowered to serve your company well in the heat of the moment.

Finally, make end user cyber security training both frequent and mandatory—company-wide. Distribute general information via email and online resources. Leverage interactive training modules to improve retention and offer employees greater convenience. Then, invest in training exercises, like phishing testing, to assess your risk and target employees who might need a little extra support—and use those opportunities to reinforce the need for them to take immediate action: shutting down their computers, disconnecting from networks, and immediately notifying IT should they ever encounter the real deal.

9. Conclusion

Reach out for expert security and data recovery support

Most organizations today are aware of the ransomware threat. Unfortunately, the gap between awareness and broad, company-wide action to mitigate the impacts of ransomware is still far too significant.

We urge you to bring your key corporate stakeholders to the table, come to a full understanding of the business threats ransomware poses, and begin development of the ransomware crisis plan that will see you safely through.

Need support?

Arcserve is always here—
standing by and ready to help.

arcserve®

+1 844 639-6792
arcserve.com