To Pay or Not to Pay?

Proven Steps for Ransomware Readiness

Crippling cyber-assaults are occurring too frequently across the globe, with consequences becoming more threatening for businesses and communities.

A question that keeps many CISOs awake at night is whether or not to pay in a ransomware attack.

In a vacuum, the guidance to withhold payment makes total sense. We don't want to negotiate with criminals. But when you need to get your business back online, a cost/benefit analysis takes effect, and a company will do what it needs to do to have continuity. Good cyber-hygiene and open discussions on possible threats and mitigation must be a focus to avoid your business getting to this point.

But if you find yourself in the dreaded situation of having to decide whether to pay the ransom, here are three top questions to consider:

1. Are you 100% sure that you need to pay in order to restore? If you already have proper data backup practices, your IT/security team may be able to restore from the latest backup.
2. What is the data worth? Figuring out what data has been crypto-locked on your devices and the data's worth to your company may make the decision for you.
3. What are you and your company willing to do from an ethical standpoint to restore that data if payment is the only option? This is perhaps the toughest and most important question to answer. In paying ransom to cybercriminals for returning your data, are you perpetuating this practice by funding the bad actors? Where will this cycle stop, and can you afford to be part of the solution?

OPPORTUNITY Vs. COST

Good security enables good business, but weak security can quickly disable operations.

Cybersecurity management is typically viewed in two ways:

1. An opportunity enabling an organization to perform, or sell better
2. A cost of goods or services sold

An organization that sees security as a business opportunity is more likely to embrace the development and implementation of good security measures. On the contrary, those that see it as a cost may be more unwilling to trade-off profit to protect their business.

> *The catastrophic attacks experienced by organizations in all corners of the globe clearly underscore the necessity for IT professionals to ensure preparedness for ransomware attacks is on top of their agenda.*
>
> — Dustin Brewer, BlueVoyant

The see-saw effect

BY GARRY BARNES, PRACTICE LEAD, VITAL ADVISORY

As companies across the globe increasingly invest in the opportunities digitization presents, balanced consideration must be given to the ratio of controls put in place to mitigate hackers.

It is easy for companies to become addicted to technology. The IT industry is designed to expedite the delivery of innovation in business. And generally speaking, new IT solutions are cheap, fast and easy to deploy, but this brings about obvious risk and gaps in security.

Introducing the see-saw effect.

As organizations invest in digitization, they are increasingly exposed to cybersecurity risk, and must balance this with preventive cybersecurity measures.

The question executives must ask is:
"How do we become the company less likely to experience a ransomware attack?"

The answer is:
"Have you put in place a balance of sufficient, adequate and effective protection over your key assets to mitigate losses and minimize risk, while also enabling your opportunities to succeed?"

Managing opportunity and cost is all about balance. How much risk is a company willing to take for an opportunity they are investing in?

Prevention better than detection

If you're not going to spend money on preventive control, you're going to be spending it on incident response.

It is true that every company using the internet has a cyber risk, just as every person driving a car takes a risk. But there is a murmur among organizations to abandon preventive controls and just prepare for the worst.

A recent ISACA cybersecurity survey found that 84% of respondents expected ransomware attacks to increase in late 2021, yet only 38% had conducted ransomware training for staff.

We have seen major advances in protective technology, but there are some basic and essential measures that must be implemented.

> *We are not at the whim of an attacker – we can head off a lot of them.*
>
> — Garry Barnes, Practice Lead, Vital Advisory

ISACA'S TOP 10 TIPS TO PREVENT A RANSOMWARE ATTACK

1. **Understand risk profiles**—Organizations should have their risk assessed to accurately prepare for potential attacks. To do this, cybersecurity teams must take inventory of responsibilities, products and services, and the technical requirements affiliated with each. By defining these risk areas, cyberteams can better assess areas that require the most attention when allocating cybersecurity resources.
2. **Realize data responsibilities**—Each employee on a cybersecurity team should realize the types of data they are responsible for storing, transmitting and protecting.
3. **Communicate clearly with executive leadership and employees**—To gain executive support, ensure that reporting and communication to the leadership level is clear and accurate. Once leadership understands the threat, the risk and its potential impacts, cybersecurity teams are more likely to receive the funding and support required to protect the organization.
4. **Comprehend organizational cybermaturity**—All points listed here are a part of comprehending an organization's cybermaturity, or its developed defensive readiness against potential cyberattacks and exploitations. Tools like the CMMI Cybermaturity Platform can help organizations understand and improve their cybermaturity.
5. **Test for incoming phishing attacks**—Most attacks start with a phishing campaign, and they continue to be effective. Try testing filters by sending yourself de-weaponized phishing emails identified by others from an external test email account. How often will they make it through? Test it. It is possible that email filters need to be strengthened.
6. **Assess all cybersecurity roles on a regular, event-controlled basis**—Regularly assess and audit cybersecurity controls to ensure that they are applied and maintained appropriately. A truly mature organization will test these controls on both a time-based schedule and in response to incidents.
7. **Evaluate patches on a timely basis**—Ensure that patches are applied in an organized and methodical fashion. For vulnerable legacy systems that cannot be patched or updated, isolate them in the network and ensure that those systems do not have access to the Internet.
8. **Perform regular policy reviews**—Make sure that all pertinent cybersecurity policies not only exist, but are also regularly evaluated and updated based on the ever-changing cybersecurity landscape. Specifically, update these policies based on both time-based schedules and event-based instances.
9. **Leverage threat intelligence appropriately**—Reading and disseminating threat intelligence throughout a cybersecurity team can be overwhelming. Hacks and cyberattacks occur on a 24/7 basis, with different branches of similar attacks emerging overnight in many instances. Understanding which type of intelligence applies to your organization and parsing it out correctly increases understanding of what threats may pose the greatest danger.
10. **Protect end-user devices**—We often forget to ensure 100% protection of end-user devices—not only for devices within the network, but for all devices used by remote users to access systems. Exclusion lists should be minimal.

> *Protecting organizations against ransomware requires a disciplined approach designed to make the adversary's mission much more difficult.*
>
> — Jesse Fernandez, CISA, CISSP, GCED, GCIH, GPEN, GSEC, GSLC

Read more:

- Protecting Your Organization From Ransomware, by Jesse Fernandez
- Cybermaturity and Protecting Against Ransomware, by Tom Conkle
- Ransomware Defense Calls for Solid Fundamentals, Rigorous Enforcement, by Chris Cooper
- CMMI Cybermaturity Platform