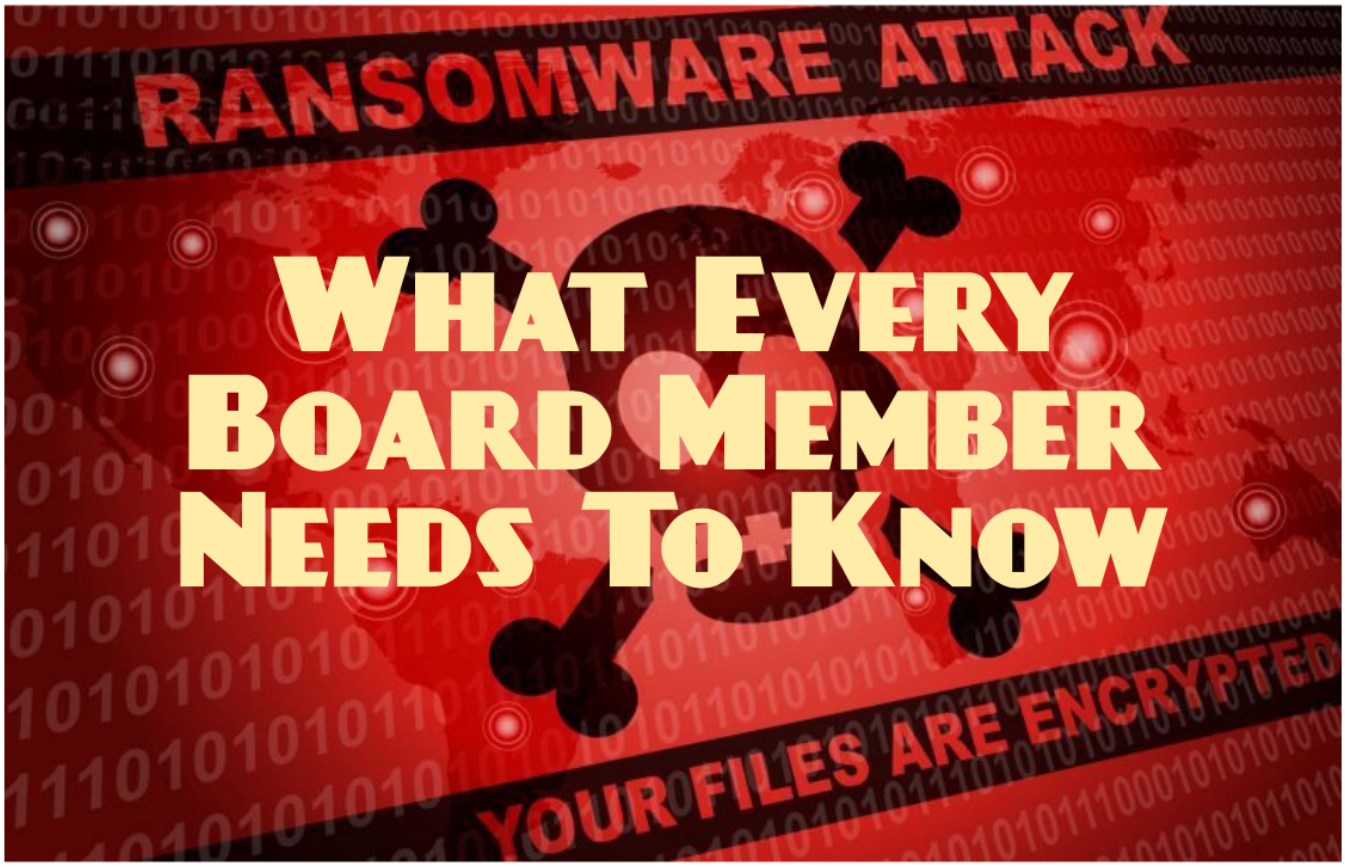
CISO ToGo
Technology Risk Consulting



… *and what they should be asking their technical/cybersecurity experts!*

The impact of a ransomware attack on an organization can be devastating. So, what should board members be doing to ensure that their organization is prepared for such an attack and be positioned to be in the best possible place to respond quickly?

This whitepaper explains the basics of ransomware and suggests relevant questions that board members might want to ask their technical/cybersecurity experts to help drive greater cyber resilience against these types of attacks.

Why should board members concern themselves with ransomware?

Cyber security is a board-level responsibility, and board members should be specifically asking about *ransomware* as these attacks are becoming both more frequent and more sophisticated.

Ransomware attacks can be massively disruptive to organizations, with victims requiring a significant amount of recovery time to re-enable critical services. These events can also be high profile in nature, with wide public and media interest.

What do board members need to know about ransomware?

Board members don't need to be able to distinguish their Trickbots from their Ryuks, but knowing the basics of how ransomware works will mean they can have constructive conversations with their technical and cybersecurity experts on the subject.

So, what do you need to know about ransomware?

- Ransomware is a type of malware that prevents you from accessing your computer (or the data stored on it). Typically, the data is encrypted (so that you can't use it), but it may also be stolen, or released online.
- Most ransomware being distributed now is 'enterprise-wide'. This means it's not just one user or one machine that is affected but often the whole network. Once they've accessed your systems, attackers typically take some time moving around, working out where critical data is saved and how backups are made and stored. Armed with this knowledge the attacker can encrypt the entire network at the most critical moment.
- The attacker will then usually make contact with the victim using an untraceable email address (or an anonymous web page), and demand payment to unlock your computer and/or access your data. Payment is invariably demanded in a cryptocurrency, such as Bitcoin, and may involve negotiation with the humans behind the ransomware (who have spent time in your organization's networks assessing how much you might be willing or able to pay).
- However, even if you do pay the ransom, there is no guarantee that you will get access to your computer or your files.
- It is also not uncommon for cyber criminals threaten to release sensitive data stolen from the network during or after the attack (commonly referred to as "double extortion ransomware").

- The US government strongly advises against paying ransoms to criminals, including when targeted by ransomware. There are practical reasons for this (***see question 4 below***), along with the concern that paying ransoms likely encourages cyber criminals to continue such attacks.

Five key questions for board members to ask about ransomware:

Q1 ... As an organization and as board members, how would we know when an incident occurred?

There is often a significant period of time (known as 'dwell time') between an attacker gaining access to your systems and the ransomware itself being launched. Identifying unauthorized access to systems early can help stop an attack, so you need to consider:

- Has the board explicitly conveyed the threshold for when it wants to be informed of an incident?
- What monitoring is in place around those critical assets (like personal data) that would have an impact if compromised, lost or changed? Bear in mind that an attacker may have gained access through non-critical systems, so regular monitoring across assets is important.
- Who examines the logs and are they sufficiently trained to identify anomalous activity?
- What mechanisms are there in place for staff to report any suspicious activity?
- Are the thresholds for alerts set to the right level (that is, are they low enough to give suitable warning of potential incidents, but also high enough so that the team dealing with them are not overloaded with irrelevant information)?
- How confident are you that you know all the IT assets that your organization has, and what the state of those assets are? Many attacks can come in via equipment that organizations are unaware of.

Q2 ... As an organization, what measures do we take to minimize the damage an attacker could do inside our network?

Ransomware attacks cause damage and can spread rapidly within your systems. You therefore might like to ask:

- How does the organization authenticate and grant access to users or systems? Are these measures hard to bypass, and is access only afforded if necessary?

- How would the organization identify an attacker's presence on the network, (e.g. is monitoring in place)?
- How is the network separated so that if an attacker gets access to one device, they will not have access to the full range of the technical estate?

Q3 ... As an organization, do we have an incident management plan for cyber incidents and how do we ensure it is effective?

Organizations should think in terms of *'when'* rather than *'if'* they experience by a significant cyber incident. So, it's essential to plan your response carefully and to practice (or 'exercise') your response.

A basic incident management plan should include:

- Identifying the key contacts (e.g. incident response team or provider, senior management, legal, PR, and HR contacts, insurance providers).
- Clear escalation routes (for example to senior management) and defined processes for critical decisions.
- Clear allocation of responsibility (specifically whether this is for normal working hours or 24/7).
- At least one conference number which is available for urgent incident calls.
- Guidance on regulatory requirements (such as when incidents need to be reported and when to engage legal support).
- Contingency measures for critical functions.
- A basic flowchart or process describing the full incident lifecycle, that can be accessed even if you do not have access to your computer systems. Likewise, you should ensure that most relevant information (e.g. incident management playbooks and resources such as checklists and contact details) are available 'offline'.

To assess the effectiveness of your plans you should also ask:

- How do we practice for cyber incidents, how often, and how do we learn from these exercises?
- What level of expertise could we call on? Have you identified an appropriately skilled company to call upon in the event your organization becomes the victim of a significant cyber-attack? Your organization may also choose to engage with such a company before any cyber security incident has taken place as part of your business continuity planning.

Q4 ... Does our incident management plan meet the particular challenges of ransomware attacks?

There are particular features of ransomware attacks that many (more general) incident management plans may not fully address. It is therefore important to discuss:

- How might we respond to a ransom demand when attackers are threatening to publish sensitive data? Who would make this decision?
  - Keep in mind (as mentioned previously) that guidance from the US government strongly advises against paying ransoms.
  - Furthermore, there is no guarantee that paying the ransom will result in a successful outcome, as it will not ensure your data is unencrypted, nor will it protect networks from future attacks or prevent the possibility of future data leaks.
- Are we prepared for a recovery that could take several weeks (with damage to corporate reputation and brand to likely last longer)?

Q5 ... How is data backed up, and are we confident that backups would remain unaffected by a ransomware infection?

Ransomware frequently targets an organization's data backups, as this increases the likelihood of an organization paying. So, it is essential that the board seek assurance on how backups are performed, how secure these are, and how frequently restoration/recovery tests are executed.

You might like to ask:

- What data is deemed as 'critical' and how frequently is this backed up?
- How frequently is non-critical data backed up?
- How confident are you that you would be able to recover from these backups? How frequently is this checked?
- How are backups stored? Are they offline and kept in a different location from your network and systems, or in a cloud service?
- Does the backup policy follow the principles outlined in our whitepaper '10 Tips To Secure Your Data Backups'?

Final Thought ...

As we have seen time and time again, the threat of ransomware is ever present and it's growing. according to an interagency U.S. government report, there have been more than 4,000 ransomware attacks every day since 2016. The response to these attacks has varied widely, with the least prepared organizations often paying the ransom demanded. And the potential damage is enormous ... according to the "State of Ransomware 2021" produced by SOPHOS, the average cost to pay a ransom is $170,404, with only 8% of those organizations managing to get back all of their data after paying the ransom!

It is clear that organizations of all sizes must put resources into building resilience against ransomware. **Having trained and experienced cybersecurity professionals available to help to guide you as you craft a reasoned strategy, while putting appropriate detection, protection, and response/recovery capabilities in place (and testing those regularly!) can prove critical to the success (or failure!) of this effort ... and this is exactly where CISO ToGo, LLC can help!**

Reach out today, to discuss exactly how we can help:

www.CISO-ToGo.com

Providing services and support throughout the United States

Email: WRichmond@CISO-ToGo.com

Phone: **401-264-0880**

because security is everyone's concern ... but it's OUR business!