K2's Understanding Your Ransomware Risk

Learning Objectives

Distinguish between various options to mitigate risk

Identify practical actions for reducing ransomware risk

List examples of high-profile ransomware attacks and how they occurred

FIRST, WHAT IS RANSOMWARE?

First, What Is Ransomware?

- Ransomware is a form of **malware** that takes control of its victim's data and holds the data hostage, typically by using a high level of **encryption**
- Once the data is encrypted, the cybercriminal demands a **ransom payment** to provide the victim with a **decryption key (or at least the promise of one!)**
  - Of course, these are criminals so there's **no guarantee** that the victim will receive the decryption key, even if they pay the ransom

A New Ransomware Trend

- A new twist on ransomware is to use the data to **exploit the victim multiple times**
  - The original ransomware attack
  - Disclosing **sensitive and private team member data** (SSNs, for example) and **corporate data** (trade secrets, customer lists, managerial compensation)
  - **Customer and client data** (tax return info)

This Is Not A New Threat

- By most accounts, **ransomware first appeared in 1989**
- Dr. Joseph Pop sent **20,000 floppy disks infected with a virus to** the World Health Organization's AIDS Conference in Sweden
- After the virus loaded onto the victim's computer and the computer was re-booted 90 times, the malware seized control of the data and **demanded a ransom of $189** be paid to a post office box in Panama

The Quiet Years Of Ransomware

- After Pop's ransomware scheme, **the exploit remained relatively benign until the late 1990s**
- At that time, would-be cybercriminals recognized that the **Internet made it much easier to transmit ransomware to unsuspecting victims**
- As such, cybercriminals began to escalate their attacks and **ransomware exploded into a very big business**

Key Stats From Ransomware.org

- Approximately **half of all businesses would pay a ransom**
- **34% have experienced an attack**, and another 14% reported that they may have experienced one
- Only 16% reported that they felt that **they were less likely to be a target**
- 84% indicated that ransomware is a **significant business threat**

- https://ransomware.org/2022-ransomware-survey/

RECENT, HIGH-PROFILE ATTACKS

San Francisco 49ers

- **BlackByte ransomware gang** was responsible for the attack
- Ironically, the attack occurred on **Super Bowl Sunday 2022**
- Data breach notifications were sent beginning August 9, 2022
- *"…we have no indication that this incident involves systems outside of our corporate network, such as those connected to Levi's Stadium operations or ticket holders"*

Cisco

- Cisco confirmed **the Yanluowang ransomware gang attacked it** on May 24, 2022
- The cybercriminals gained access to an employee's credentials through a **compromised Google account where credentials had been saved in a web browser**
- The attacker used **voice phishing attacks to convince the victim to accept multi-factor authentication push notifications**, which provided access to the VPN

Los Angeles Unified School District

- **Vice Society** claimed responsibility for a September 5 attack on LAUSD…the attack occurred just days before the start of the new school year
- LAUSD declined to pay the ransom
- In October 2022, Vice Society claimed responsibility for the attack and posted the stolen data on the Dark Web

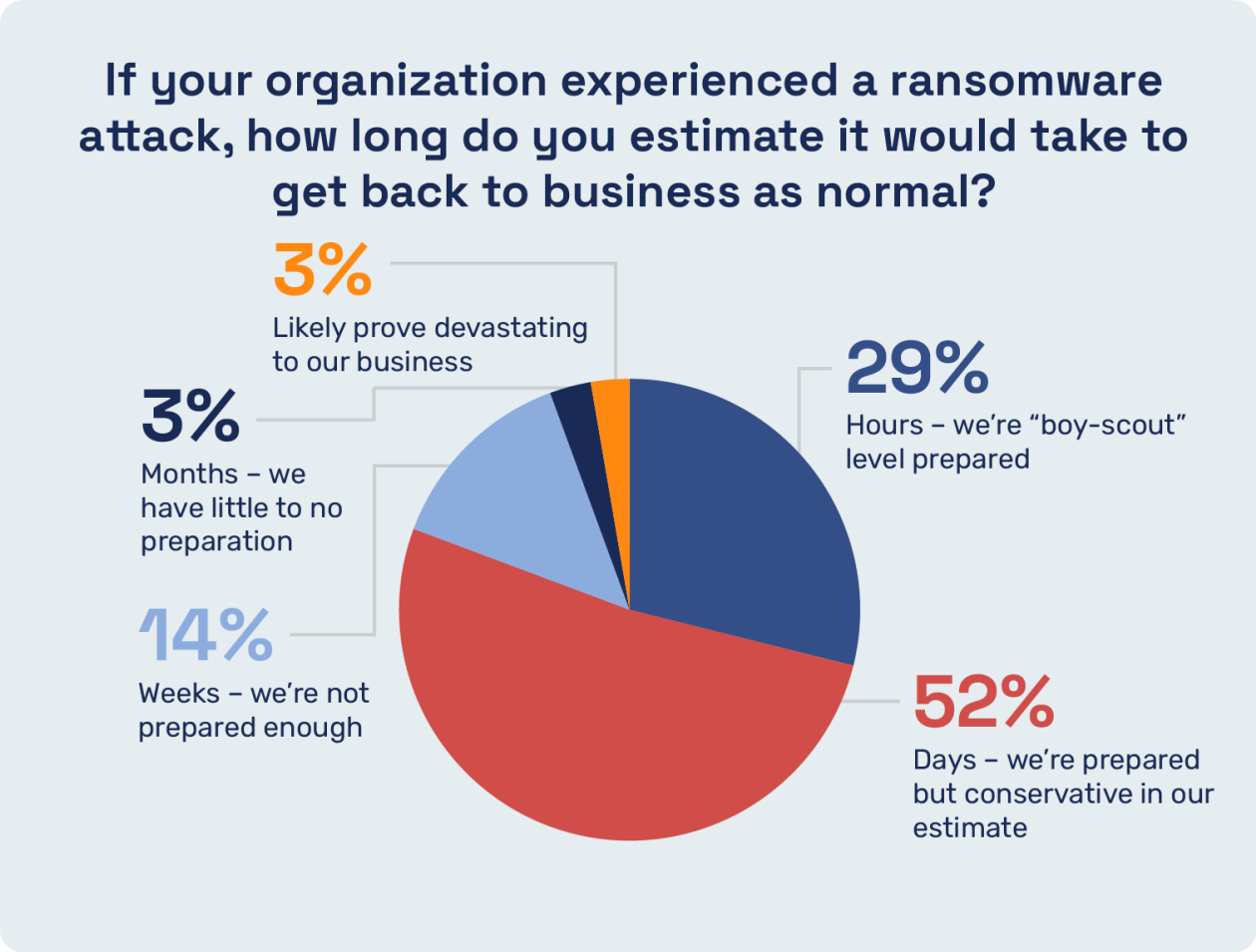
Rackspace Technology

- In December 2022, **Rackspace was victimized in an attack that caused widespread outages of its hosted Exchange services**
- Because customers could not access their email, **Rackspace migrated affected customer accounts to Microsoft 365**
- Rackspace has not commented on whether it paid the ransom

Colonial Pipeline

- **Colonial Pipeline** – a major petroleum pipeline company in the Southeastern portion of the US – **was victimized in May 2021**
- The attack caused **massive disruption in the distribution of fuel** throughout the Southeast
- Initially, the **hackers demanded $100 million in ransom**
  - **Initially, Colonial refused to pay, but ultimately paid approximately $5 million** on the belief they could recover more quickly
- Contributing to the attack was the use of **"legacy" software that did not support multi-factor authentication**

Are You And Your Team Prepared For What Might Be Inevitable?



Source: www.ransomware.org

UNDERSTANDING WHERE YOUR RISK IS

Major Ransomware Attack Vectors

- Email attachments and links
- Social engineering
- Remote Desktop Protocol (RDP)
- Managed Service Providers (MSPs)
- Drive-by downloads

Email Attachments And Links

- **Don’t Do It!!! Don’t click on the link or attachment unless you were expecting it and know who sent it to you…easy to say, but we’re only human, and we will make mistakes!**
- Therefore, **ratchet up email security** to call attention to the fact that a message with a **link or attachment came from someone outside the organization**
- Consider “**stripping” all attachments from inbound messages originating outside the organization**
- And, of course, **enable strong anti-malware tools**

Social Engineering

- **Social engineering attacks attempt to trick someone into performing an action that they know they should otherwise not do**, such as surrendering a password to an unknown team member posing as someone on the IT staff
- A common form of social engineering is "**vishing**" (voice phishing)
  - For example, pretending to be an IT manager who needs your username and password so they can perform some "maintenance." Instead, they are trying to harvest info they can use to precipitate a ransomware attack…DON'T DO IT!!!!

Remote Desktop Protocol

- RDP is a means of remotely accessing another device
- Unfortunately, **RDP is also one of the most common attack vectors used to deploy ransomware**
- If you're going to use RDP, **consider changing the default port way from 3389**
- Also **ensure that sound MFA controls are in place**
- Remember, if a hacker can get into your system through RDP, they can easily deploy ransomware

Managed Service Providers

- Carefully choose your MSPs and **thoroughly vet them and their cyber insurance policy**
- **Ensure their policy is sufficient given the size and scope** of their operations
- ***Will proceeds be available to help remedy your data in the event of a ransomware attack***?

Drive-By Downloads

- Drive-by downloads can occur when you visit a website that exploits a **weakness in your browser, plugins, or other tools**
- In this case, you can become a victim without necessarily doing anything wrong…you just visit a compromised website, and you become a victim
- Obviously, **carefully choose which websites you visit**!

COMMON SENSE RISK REDUCTION STEPS TO REDUCE RANSOMWARE'S THREATS

Team Member Education

- **Ensure team members understand the threats** associated with ransomware and how it could impact them personally
- Consider using the “test phishing” resources available from companies like **PhishMe** and **KnowBe4**…if you’re a Microsoft 365 company, you can send tests through **Exchange Online**
- Follow up these tests with **appropriate educational efforts and, if necessary, disciplinary actions**

Log In With “Standard” Rights

- As a matter of course, users should not log in with **Admin** rights because doing so elevates the chance that ransomware can install and run
- Therefore, always log in with **Standard** rights instead
  - If you have Admin rights and find that you need to perform an action that requires Admin rights, you can “elevate” your privileges using Windows’ **User Account Control**
- **Further, enable extra layers of protection on privileged roles,** including IT administrators to make it more difficult for a widespread attack to occur

Take Advantage Of CFA

- **Controlled Folder Access (CFA) is a Windows feature designed to limit the impact of a ransomware attack**
- When you enable CFA, you reduce the potential impact of a ransomware attack because you can designate certain folders on your device as “protected”
- **Data stored in protected folders can only be changed by pre-authorized applications**, which presumptively would not include the ransomware load; therefore, your data may likely be unaffected by a ransomware attack

Prepare For The Worst!

- Despite the controls outlined, **there are no guarantees that your company will remain unaffected by ransomware**
  - Therefore, **assume that, at some point, you will become a victim**
- If you are victimized, **can you recover all your data from your backup drives, tapes, clouds, etc.?**
  - Are you ***SURE***?
- Ensure your backup strategy includes a **proper mix of on-site and cloud-based backups, with appropriate "air gaps"** in place
- Further, **test your backups periodically**!

Summary

- Ransomware is not new, but individuals and organizations continue to become victims every day
- And when ransomware strikes, the costs can be exorbitant, possibly to the point of forcing an entity out of business
- Yet, effective internal controls can reduce ransomware's risk, for individuals and organizations alike
- Take advantage of the controls outlined in this session to minimize the chance that you will become another victim