RSA® Conference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **CXO-M03**

The Reason Companies Fall Victim to Ransomware Isn't What You Think

David S. Langlands

Vice President, Security Offerings
DXC Technology
@zerodave

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

The Wake-Up Call—A Ransomware Case

image: Quino Al / Unsplash

The first 48 hours…

- Chaos reigns supreme
- Teams and resources being stood up
- Unclear if threat actors are still active
- No one is sleeping
- Gaps immediately appear in preparedness and skills

What We'll Cover Today:

- Three recent ransomware incidents from the CxO's perspective
- Key similarities and takeaways
- Key mistakes organizations make when looking to combat the threat of ransomware
- What executives should ask for to reduce the impact and speed of recovery from similar threats

Why Staying Secure Is Getting Much Harder

OVERWHELMING COMPLEXITY

On premise, public cloud, hybrid cloud, multi cloud, SaaS, containers….

IT is changing too fast for security to keep up.

GROWING THREAT

The adversary is getting smarter and has developed a sophisticated ecosystem to monetize development, deployment and execution of ransomware campaigns.

Ransomware as a service is driving high volume attacks.

FAILING AT THE BASICS

Most of the breaches we see start with a failure of basic security hygiene.

You don't necessarily need more security products.

You can successfully deal with the threat by tackling the basics and using capabilities you may already have.

The Statistics Suggest We're Struggling…

435%
Increase in ransomware attacks since 2020 Deep Instinct

60% of breaches involved vulnerabilities for which a patch was available but not applied CSO

4X
projected increase in supply chain attacks in 2021 ENISA

46%
Increase in attacks against OT devices in 2021 Outseer

100s of Businesses from Sweden to U.S. affected by Kaseya Cyberattack

$2.3M The amount in digital currency recovered from ransom paid by Colonial Pipeline

Ransomware "business" is growing. Ransomware as a Service gangs continue to gain clients and provide software for more attacks

$11M Amount JBS Holdings is said to have paid in ransomware after recent attack

Key Lessons from the 1st Incident

- Enable multi-factor authentication for external access
- Map your key terrain – know thyself
- Practice your cyber incident response

404 Error: File Not Found—Our Second Case

image: Claudio Schwarz/ Unsplash

When your business is data…

- You care a lot about backups…
- And restoring data is a practiced skill…
- But recovering all your data at once?
- Customers have tough questions
- Interdependencies between systems can cause significant delays

Key Lessons from the 2nd Incident

- Practice your cyber incident response
- Test your recovery time with backups
- Map your key terrain – know thyself

Pandemic Pandemonium: Our Final Case

image: Martha Dominguez de Gouveia / Unsplash

Lives are at stake…

- Electronic health records are offline
- Care limited to emergency-only
- Patients are being redirected
- Media pressing for answers
- Lack of pre-planning can lead to months of time for recovery

Key Lessons from the 3rd Incident

- Train your staff to recognize suspicious attachments
- Plan for recovery and resilience, not just response
- Check your cyber insurance policy

What We Covered:

- Three incidents with similar avoidable causes
- Simple cyber hygiene recommendations to speed recovery
- The requirement to balance people, process and technology (no silver bullets)
- What executives should ask for to reduce the impact and speed of recovery from similar threats

Apply What You Have Learned Today

- Next week you should:
  - Ask when the last time your incident response plan was tested
  - Check your cyber insurance policy for proper coverage and exclusions
  - Ensure critical information needed for recovery is available offline
- In the first three months following this presentation you should:
  - Identify and eliminate all non-multifactor access to your network and applications
  - Regularly train your users using targeted phishing simulations
  - Execute a full incident response, recovery, and restoration simulation
- Within six months you should:
  - Test the effectiveness of your endpoint, e-mail, and cloud controls against real-world threats
  - Regularly check your endpoints, network, and cloud for vulnerabilities / misconfigurations
  - Implement lessons learned from your response simulations to focus on resiliency

Questions?

RSA®Conference2022

Thank You!

David S. Langlands
DXC Technology

@zerodave