Principles of Ransomware

October 4, 2022

Course Agenda

- Introductions
- Ransomware Case Study
- Ransomware Overview
- Common Attack Vectors
- Infection Stages
- Planning for Ransomware
- Cyber Liability Insurance
- Business Impact Assessment
- Ethical and Legal Considerations
- Risk Management Strategies
- Template and Checklist Resources

Introductions

About Heather Engel and Strategic Cyber Partners

- Founder and Managing Partner at Strategic Cyber Partners, an advisory and consulting firm based in Hampton Roads, Virginia.
- Advises clients across industries on risk management, IR and contingency planning, compliance, and security program development.
- Recognized subject matter expert in DoD cybersecurity, NIST frameworks, FedRAMP, and Payment Card Industry security standards.
- Frequent author and speaker on cyber security topics of interest with multiple industry certifications.

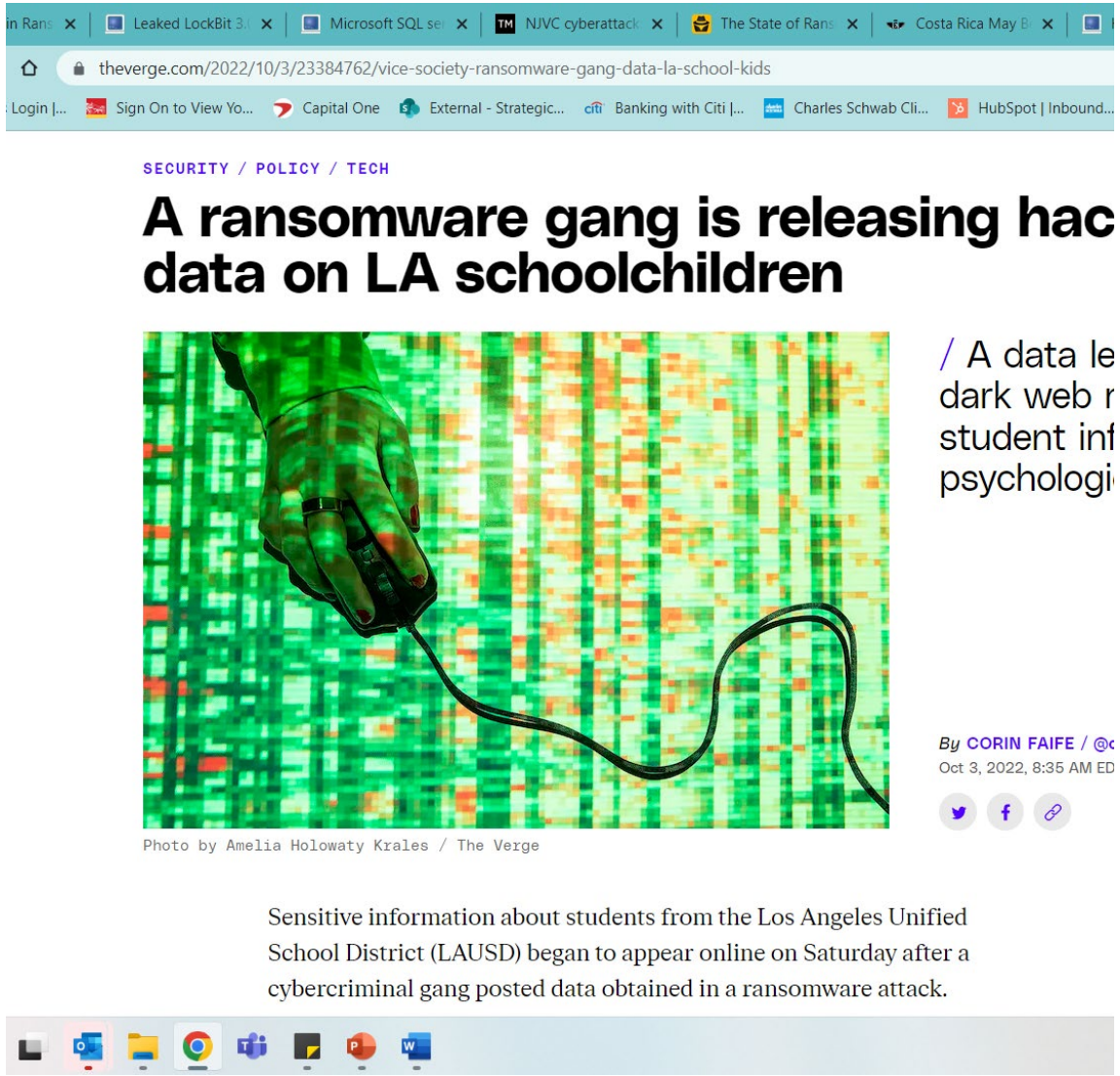
STRATEGIC CYBER PARTNERS

Participant Introduction

- Name/Company
- Role
- What do you hope to get out of this course?

LAUSD Case Study

- “The stolen data was posted to Vice Society’s dark web leak site and appears to contain personal identifying information, including passport details, Social Security numbers and tax forms. While TechCrunch has not yet reviewed the full trove, the published data also contains confidential information including contract and legal documents, financial reports containing bank account details, health information including COVID-19 test data, previous conviction reports and psychological assessments of students.”



Discussion Questions

- Why would the attackers release data ahead of the deadline?
- How could LAUSD have prevented this?
- What is the impact of the release?
- Why would a school make an attractive target?
- What questions do you have about this case?

Costa Rican Government Case Study: Double Jeopardy

- On April 17, 2022 Conti attacked nearly 30 institutions of the CR Government.
- The government had to shut down the computer systems used to declare taxes and for the control and management of imports and exports, causing losses to the productive sector on the order of US$30 million per day.
- On May 31, 2022, Hive attacked the CR Social Security Fund. (Ransom: $5m BTC = $95B USD)
- 4,871 users missed their medical appointments on the first day, another 12,000 missing appointments the next day.

Discussion Questions

- Could this attack have been prevented?
- What are some potential motivations behind this attack?
- If you were working on this response, what questions would you have based on the information given?

Break
10 minutes

Ransomware: An Overview

What is Ransomware?

- Malicious software
- Has the ability to encrypt files
- Asks for payment in exchange for decryption key

<u>Most often has multiple payloads:</u>

- Encryption
- Exfiltration
- Credential Stealing
- Individual Extortion
- Spear Phishing of partners and suppliers
- DDoS Attack
- Reputational Damage

Ransomware Characteristics

- Fake or Actual
- Immediate Action vs. Delayed
- Automatic or Human Driven
- One device or Multiple
- File Encryption vs Boot Infection
- Good Encryption vs Bad

Common Attack Vectors

Exploit Methods

- Social Engineering
- Misconfigurations or Insecure Configurations (RDP is most common)
- Software Error
- Eavesdropping/Man-In-The-Middle
- Data Packet Malformation
- Insider Attack
- Third Party Pivot
- Physical Access

Infection Stages

How an Attack Evolves

- Infiltration/Initial Compromise
- Establish Command and Control
- Auto Update
- Location and Language
- Waiting and Reconnaissance
- Exfiltration
- Encryption
- Extortion
- Negotiation
- Key Exchange
- Data Release

Break
10 minutes

Planning for Ransomware

Who is part of your Crisis Response Team?

- Incident Response Coordinator
- IT and IT Security
- Threat Intelligence/Ransomware SME
- Legal
- Finance
- Communications/Media
- Executives
- Forensics
- External Agencies
- Insurance

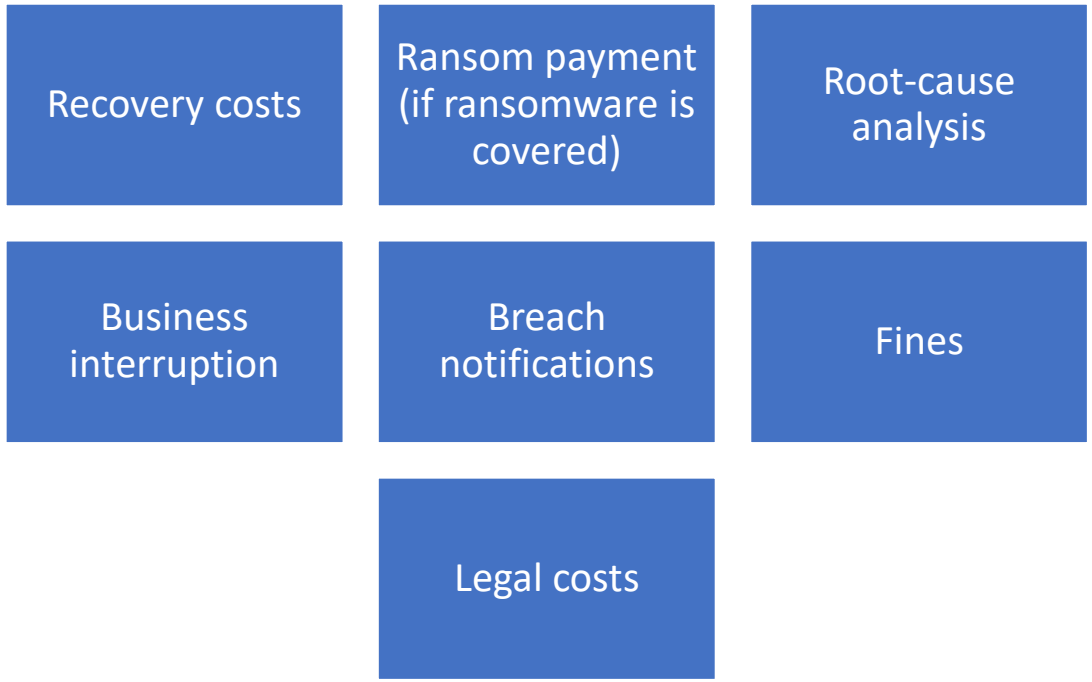
Cyber Liability Insurance

Cyber Insurance

- Standard Clauses vary widely between underwriters
- Lots of exclusions or “gotchas”
- Many policies change every year
- Do you need it?

Obtaining Cyber Insurance

Most policies cover…



But beware of…

- Changes in coverage from year to year
- Exclusions
  - Employee error
  - Social engineering
  - Lack of compliance
  - Terrorist acts and war exclusions
  - Work from home scenarios

Business Impact Assessment: Consider All the Costs

- Ransom and Negotiation Brokering
- Mitigations
- Labor Resources
- Third Party Assistance
- Business Interruption Expenses
- Law Enforcement, Investigative Costs, Prosecution
- Fees and Fines
- Reputational Risk
- Retention Cost
- Legal Costs

Ethical and Legal Considerations

Paying the Ransom May Not Be an Option

- Country of Origin
- Sanctions on Ransomware Attack Groups
- Regulatory Restrictions
- Cultural Considerations
- Reputational Risk

Facilitating Ransomware Payments on Behalf of a Victim May Violate OFAC Regulations

Under the authority of the International Emergency Economic Powers Act (IEEPA) or the Trading with the Enemy Act (TWEA),[12] U.S. persons are generally prohibited from engaging in transactions, directly or indirectly, with individuals or entities ("persons") on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of

---

OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC. OFAC's Economic Sanctions Enforcement Guidelines (Enforcement Guidelines)[13] provide more information regarding OFAC's enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation. Enforcement responses range from non-public responses, including issuing a No Action Letter or a Cautionary Letter, to public responses, such as civil monetary penalties.

Paying the Ransom

- Engage your legal team
- Legal handles all outside communications
- Determine whether the attacker is on a banned watch list
- Involve law enforcement
- Preserve evidence
- Determine if the ransomware constitutes a data breach
- May use a third-party negotiator

Risk Management Strategies

User Training

- Social Engineering is a leading cause of data breaches
- Conduct regular and in-depth user training on cyber security awareness
- Train users to recognize and report phishing emails

IRP Development, Training, and Exercise

Other Risk Management Techniques

- Vigilance in patching
- Use a SIEM
- Use MFA
- Data Encryption
- Consider more advanced techniques like FSRM, Zero Trust architectures
- Secure remote access
- Secure configurations
- Application control (block/deny all)
- Segmentation on networks
- Enable a foreign language

Resources

Cyber Playbook Template

Ransomware Resource Checklist

Questions and Discussion

STRATEGIC CYBER
PARTNERS

ICMC
THE INTERNATIONAL CRISIS MANAGEMENT CONFERENCE

Heather Engel

Heather.engel@strategiccyberpartners.com

757-250-7485

StrategicCyberPartners.com

linkedin.com/in/heather-engel-5559335/