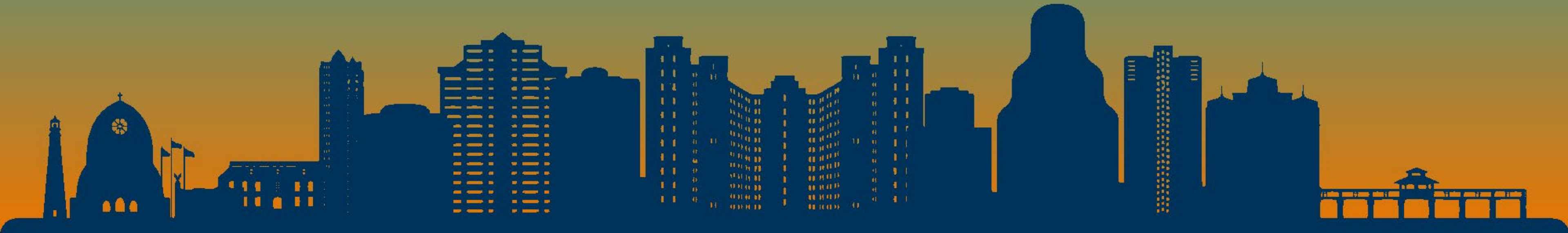
David Lam, Jason Gotway, John Rostern

June 11, 2024

Face Your Worst Nightmare: A SECURITY HACK!

LEA GLOBAL NORTH AMERICAN REGIONAL CONFERENCE



Today

- Setting the Stage
- Your laptop (attack)
- The Phishing Attack
- Takeaways

Curious QR Codes

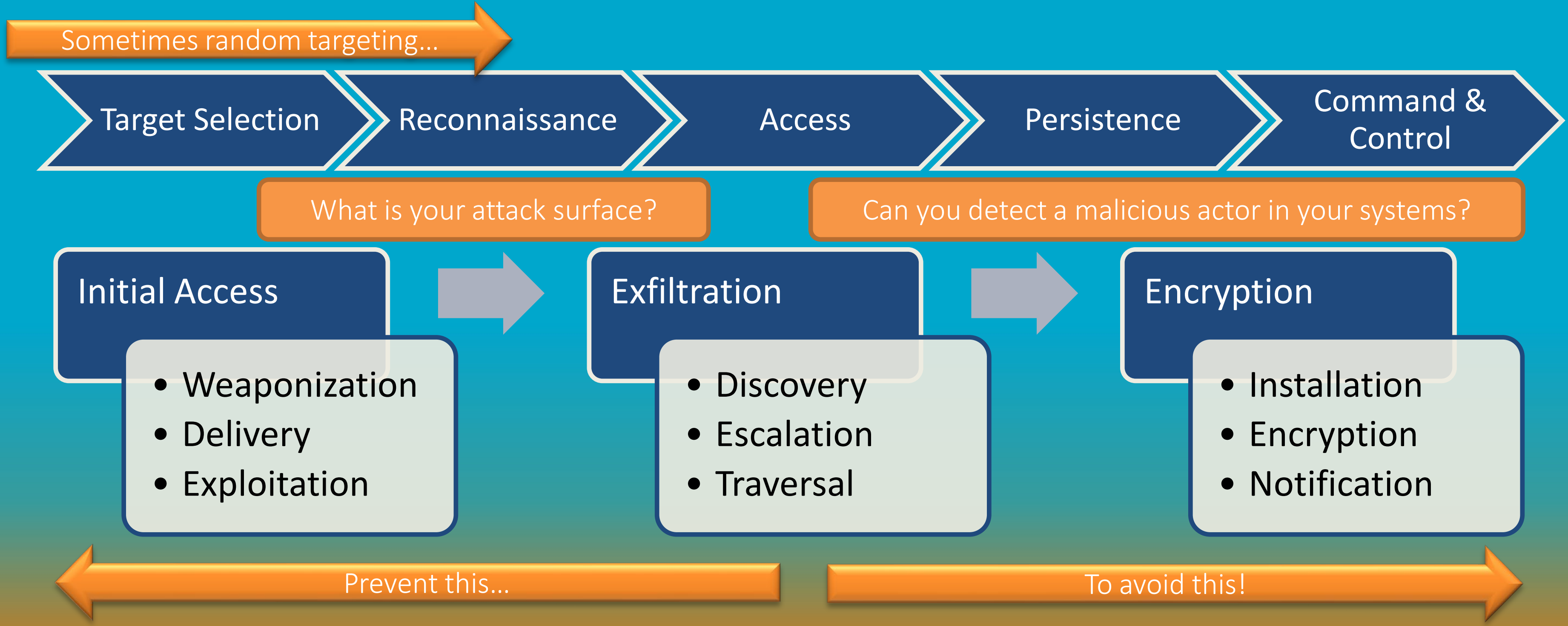
Setting the Stage

- Heightened cyber threat environment due to geopolitical unrest (Ukraine, Gaza, China, etc.)
- Continued increase in cyberattacks – particularly ransomware
- Increased attacks on critical infrastructure and industrial control systems (power grid, water supply, telecommunications, healthcare, etc.)
- Easy availability of nation-state grade ‘hacking’ tools including those available ‘as a service’
- The rapid adoption of Artificial Intelligence (AI) and it’s impact on cybersecurity in terms of both defense and offense
- Increased regulatory requirements in the US regarding the reporting of data breaches and cyber attacks

Laptop Demo

Volunteers?

Ransomware Attack Kill Chain



Sometimes random targeting…

Target Selection → Reconnaissance → Access → Persistence → Command & Control

What is your attack surface?

Can you detect a malicious actor in your systems?

Initial Access

- Weaponization
- Delivery
- Exploitation

Exfiltration

- Discovery
- Escalation
- Traversal

Encryption

- Installation
- Encryption
- Notification

Prevent this…

To avoid this!

Common elements in successful cyber attacks:

Attack Vectors

- Phishing
- Malware
- Third-Party Compromise
- Employee Errors

Vulnerabilities

- Deprecated or unpatched systems
- Lack of effective data encryption
- Lack of Third-Party risk management
- Software Security – failure to require secure coding and development practices
- Lack of employee security awareness

What you need to do…

What you need to do…

People

- Awareness
- Phishing simulations
- Reminders
- Training on processes and systems
- Acknowledgment of policies
- Consequences

Phishing Demo

- Volunteers?
- Assessing the email.
- Typosquatting
- Clicking on the link.
- What do you do next?

What you need to do…

Management

- Documented Policies
- Governance program
- External review
- Meet regularly
- Lead from the top
- Understand your information assets
- Assess third parties, including software development

What you need to do…

Technology

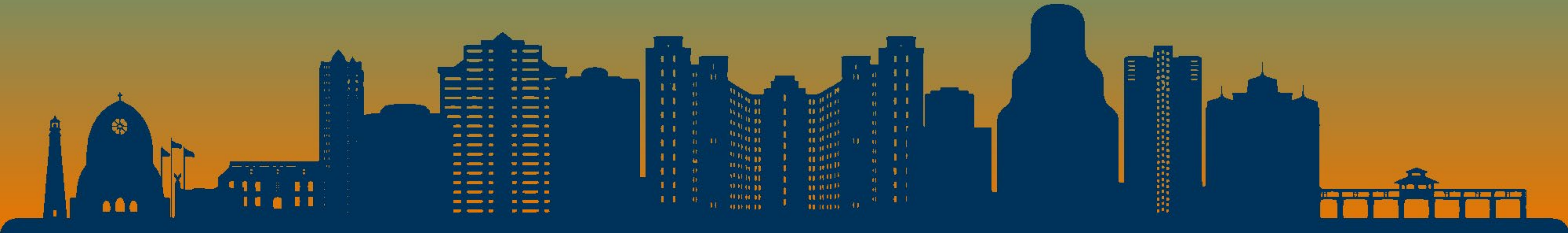
- Vulnerability scans
- Multifactor Authentication (MFA)
- Managed Detection and Response
- Manage your backups and make them immutable
- Get a password vault
- Encrypt your data

Most important take aways:

Set your intention

Make continual, reasonable progress.

Must be demonstrably effective and fiscally practical.



Questions