nisc
Cybersecurity
Services SM

1

nisc
Cybersecurity Services

Scott
KAYLOR
Senior Manager
Professional Services

nisc

2

nisc
Cybersecurity
Services

3

nisc
Cybersecurity
Services

4

nisc Cybersecurity Services

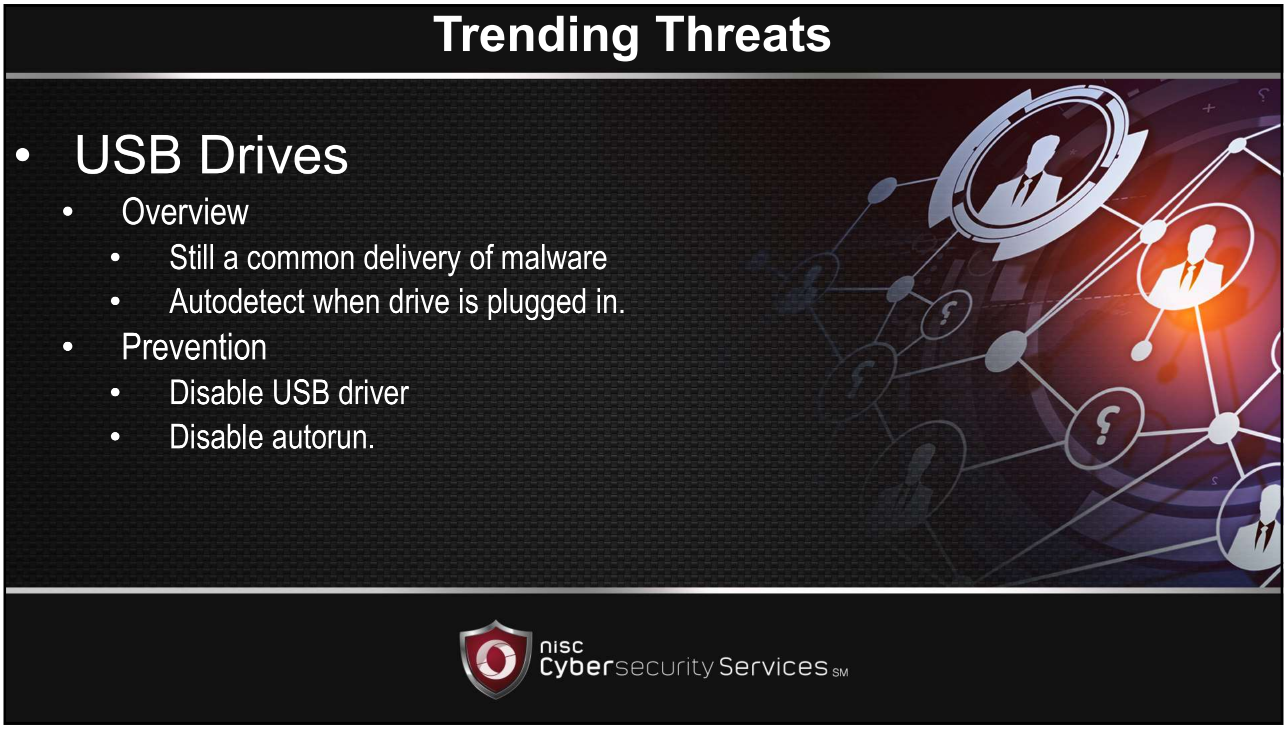
5

Agenda

- Trending threats
- Industry Cyber Events
- Cyber Tools

nisc Cybersecurity Services

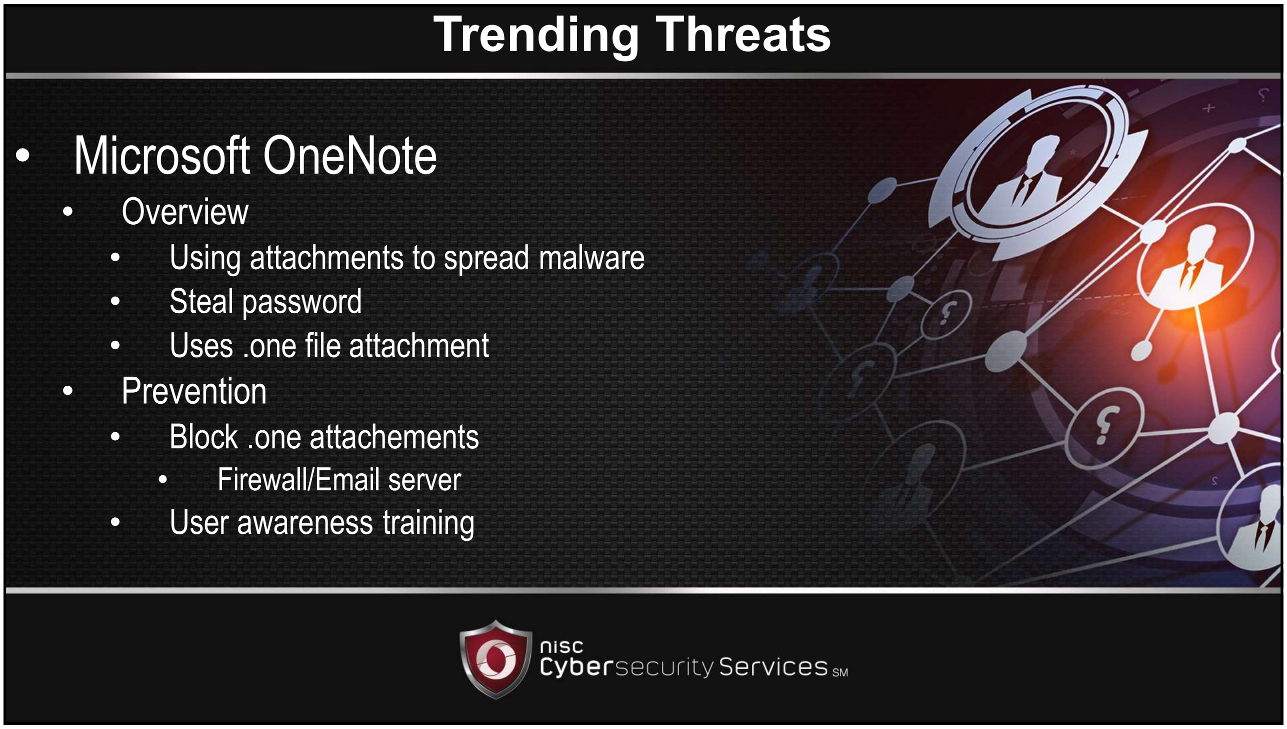
6



Trending Threats

- USB Drives
  - Overview
    - Still a common delivery of malware
    - Autodetect when drive is plugged in.
  - Prevention
    - Disable USB driver
    - Disable autorun.

7



Trending Threats

- Microsoft OneNote
  - Overview
    - Using attachments to spread malware
    - Steal password
    - Uses .one file attachment
  - Prevention
    - Block .one attachements
      - Firewall/Email server
    - User awareness training

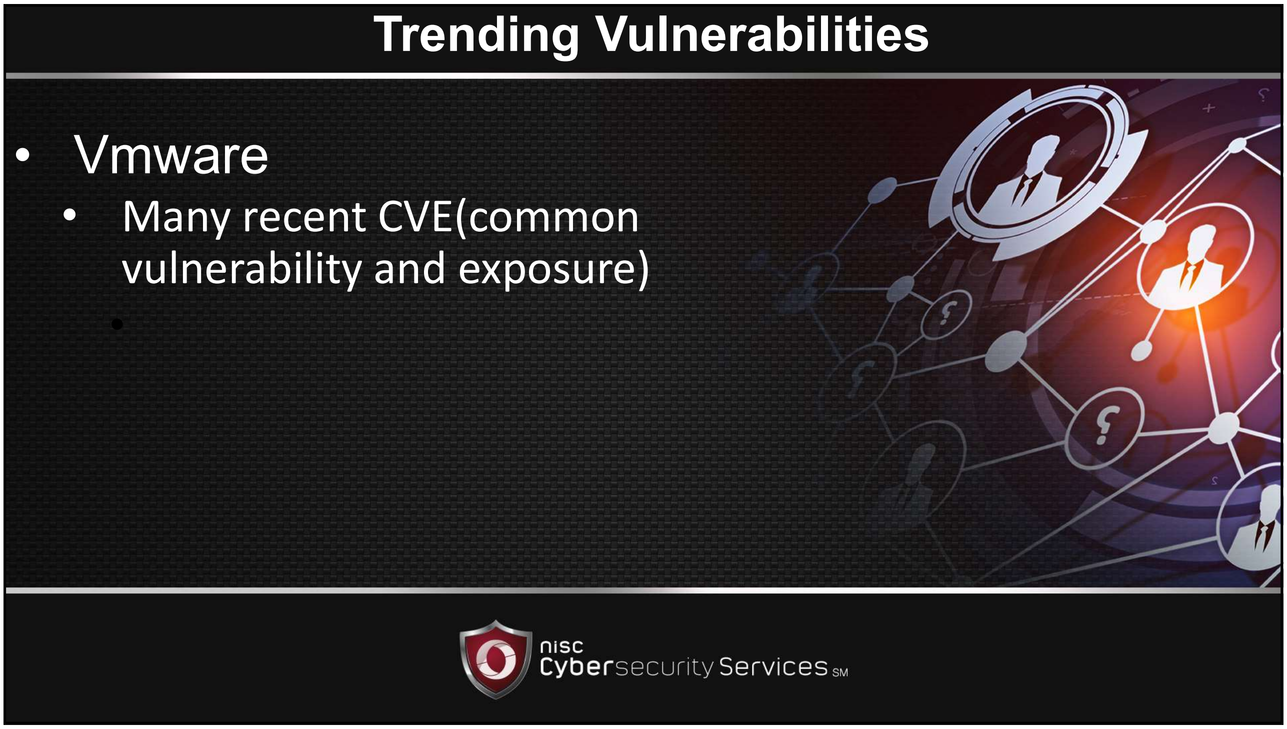
8

Trending Threats

- MFA
  - Overview
    - Continue rise in credentials stolen
    - No MFA on VPN, VDI, SaaS
  - Prevention
    - Harden MFA to prevent push fraud
    - User training
- Attacker are banking on alert fatigue

nisc Cybersecurity Services SM

9

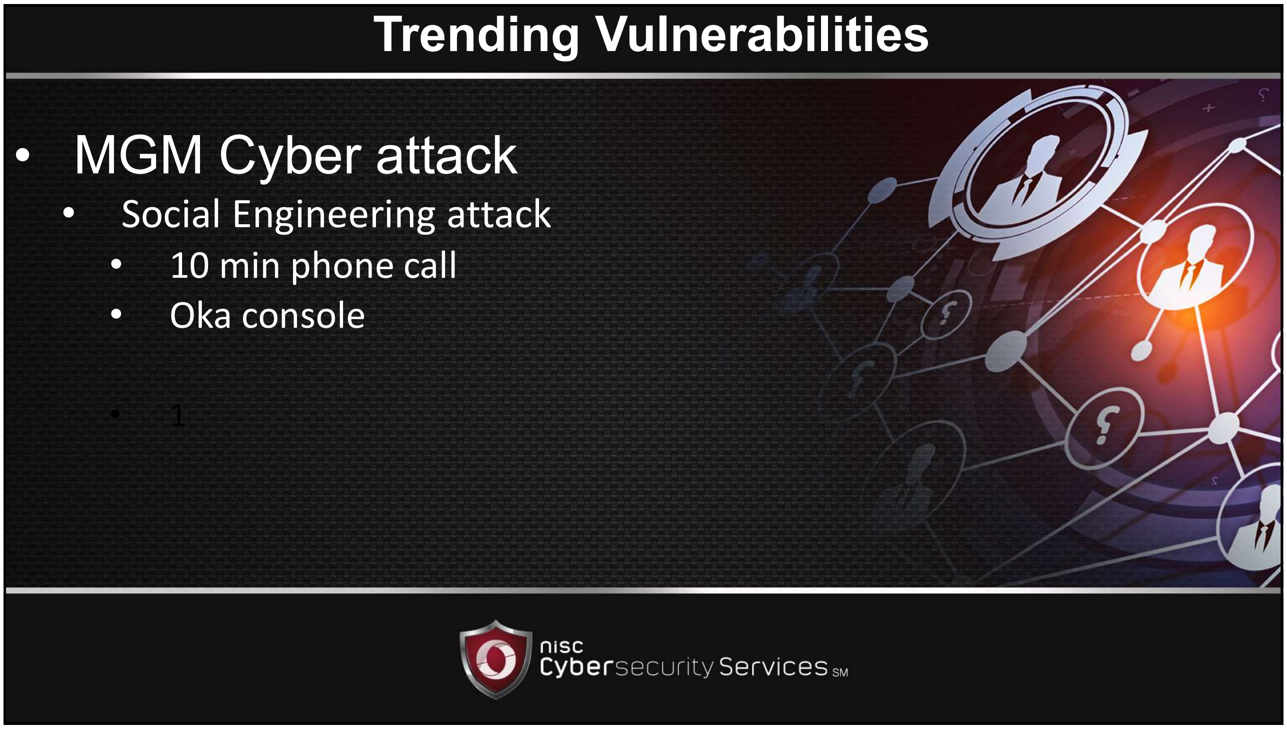


Trending Vulnerabilities

- Vmware
  - Many recent CVE(common vulnerability and exposure)

nisc Cybersecurity Services SM

10

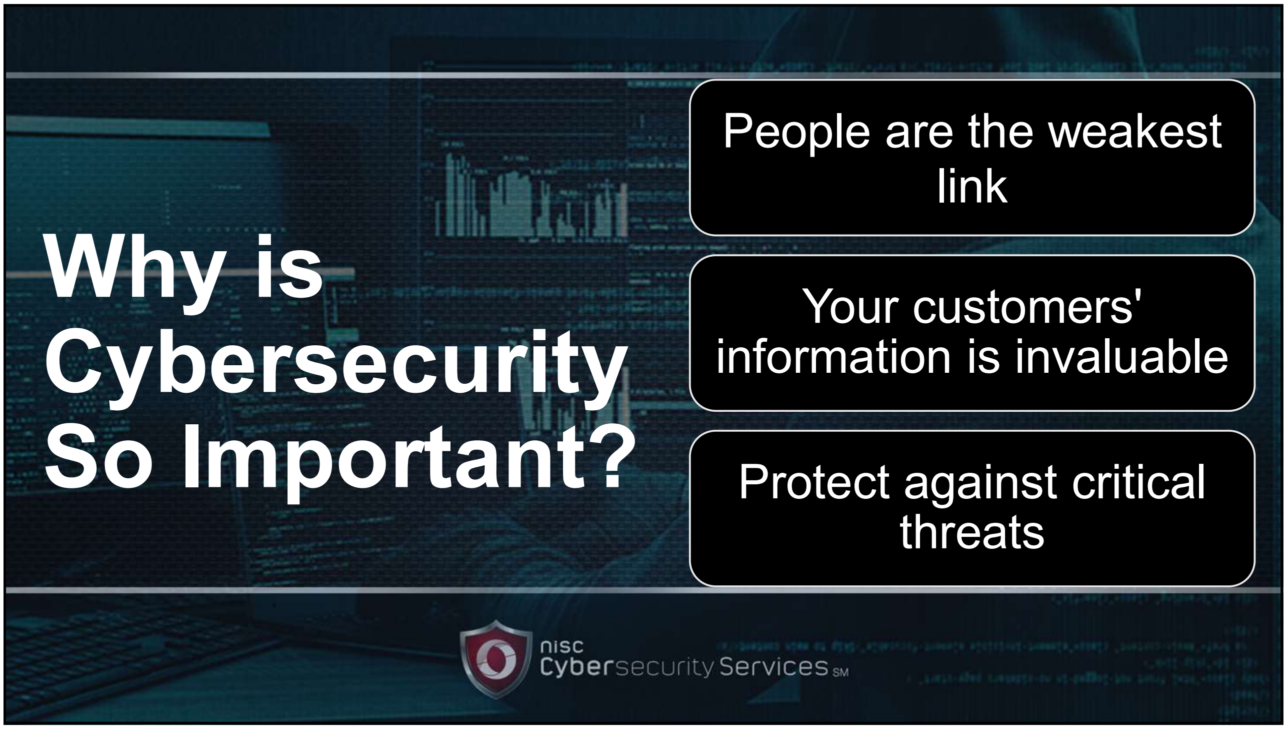


Trending Vulnerabilities

- MGM Cyber attack
  - Social Engineering attack
    - 10 min phone call
    - Oka console
    - 1

nisc Cybersecurity Services SM

11



Why is Cybersecurity So Important?

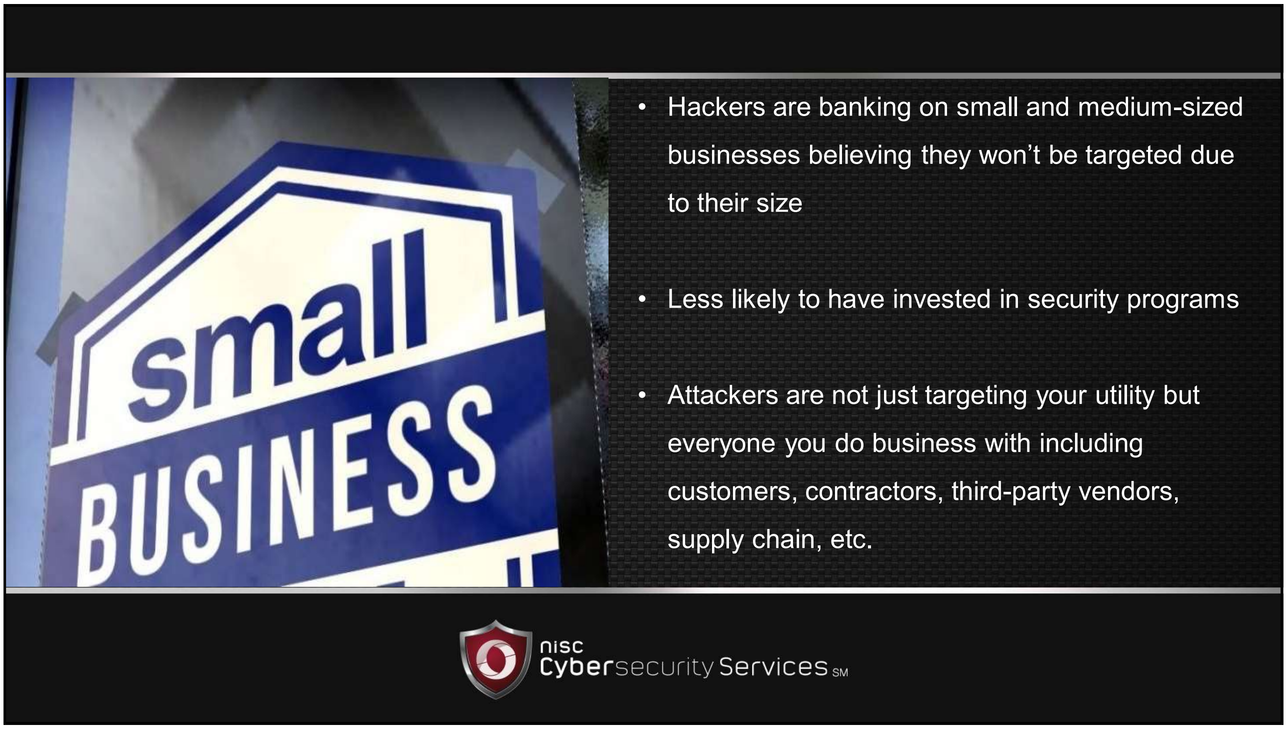
People are the weakest link

Your customers' information is invaluable

Protect against critical threats

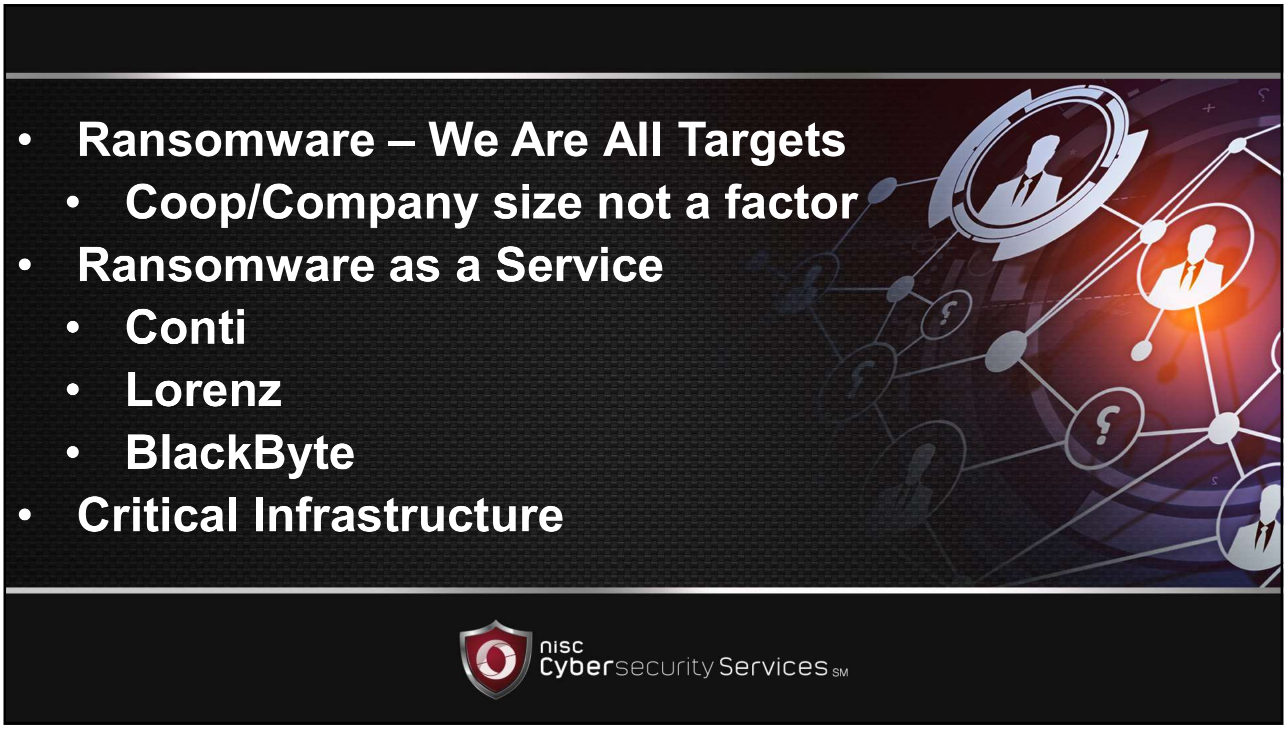
nisc Cybersecurity Services SM

12


small
BUSINESS
nisc Cybersecurity Services SM

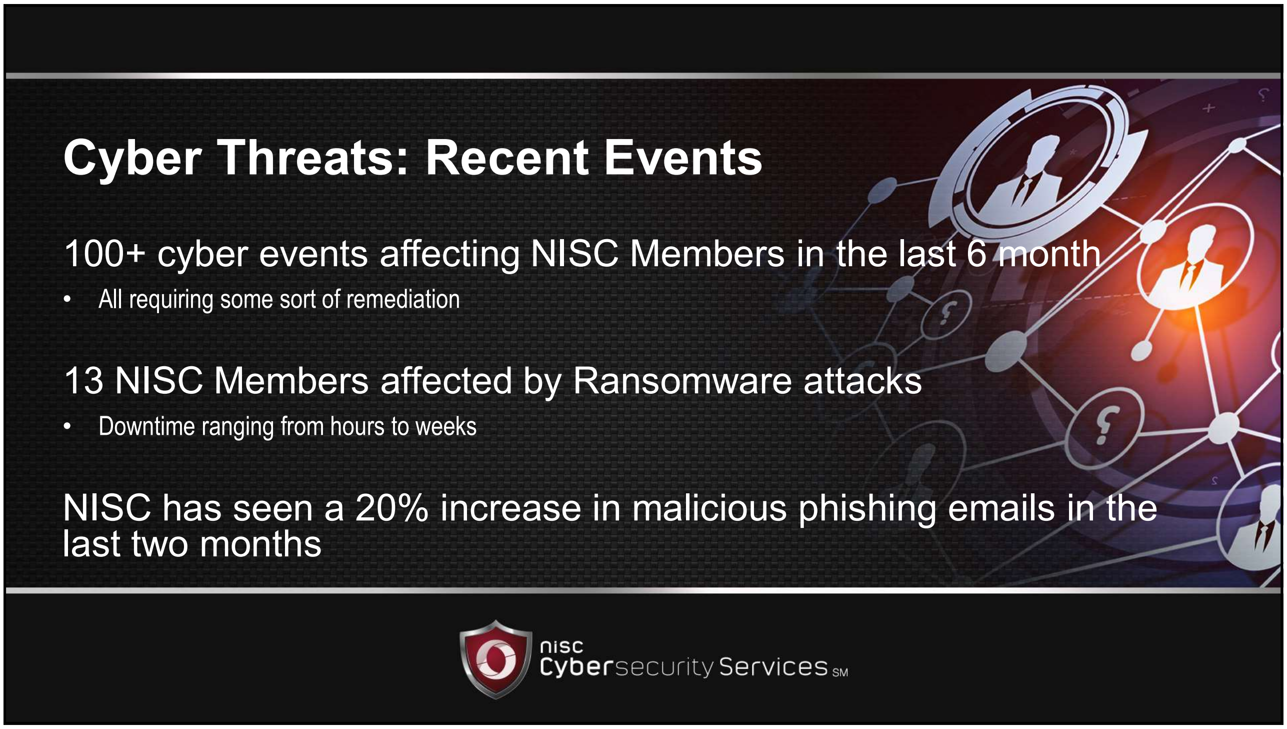
- Hackers are banking on small and medium-sized businesses believing they won’t be targeted due to their size
- Less likely to have invested in security programs
- Attackers are not just targeting your utility but everyone you do business with including customers, contractors, third-party vendors, supply chain, etc.

13


nisc Cybersecurity Services SM

- **Ransomware – We Are All Targets**
  - **Coop/Company size not a factor**
- **Ransomware as a Service**
  - **Conti**
  - **Lorenz**
  - **BlackByte**
- **Critical Infrastructure**

14



Cyber Threats: Recent Events

100+ cyber events affecting NISC Members in the last 6 month

- All requiring some sort of remediation

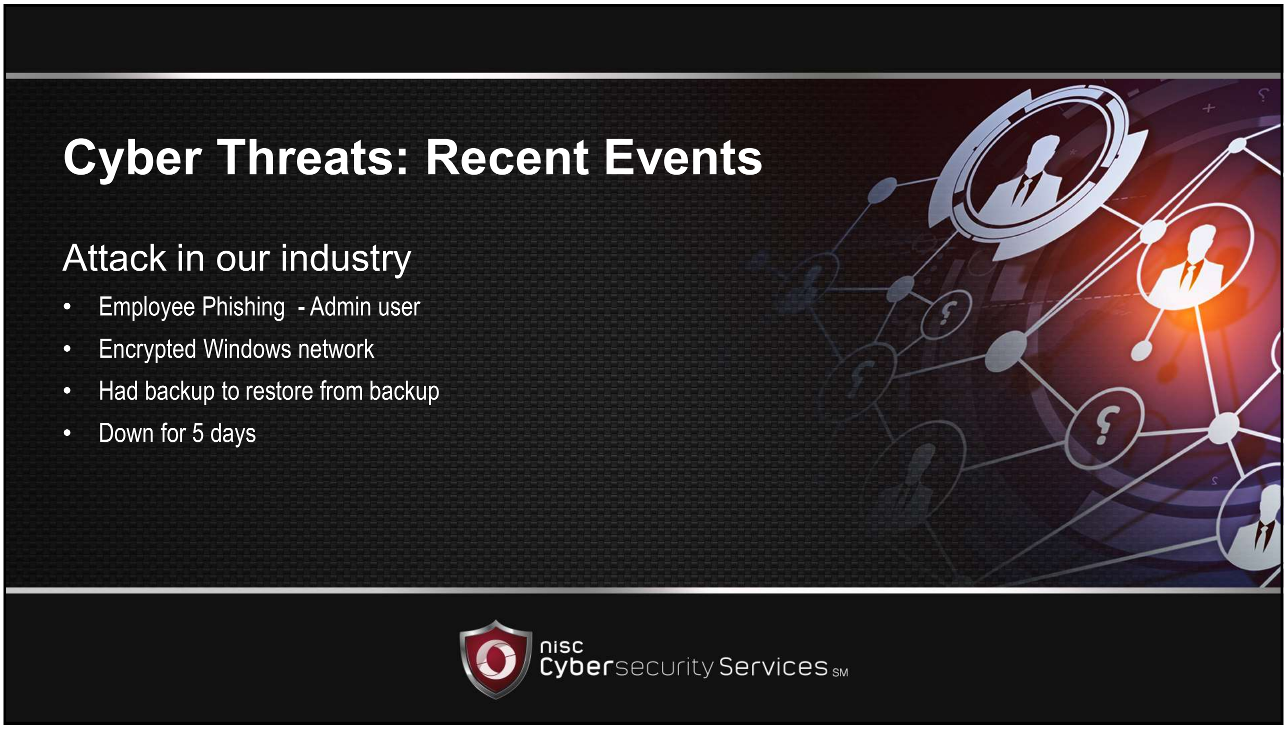
13 NISC Members affected by Ransomware attacks

- Downtime ranging from hours to weeks

NISC has seen a 20% increase in malicious phishing emails in the last two months

nisc Cybersecurity Services SM

15



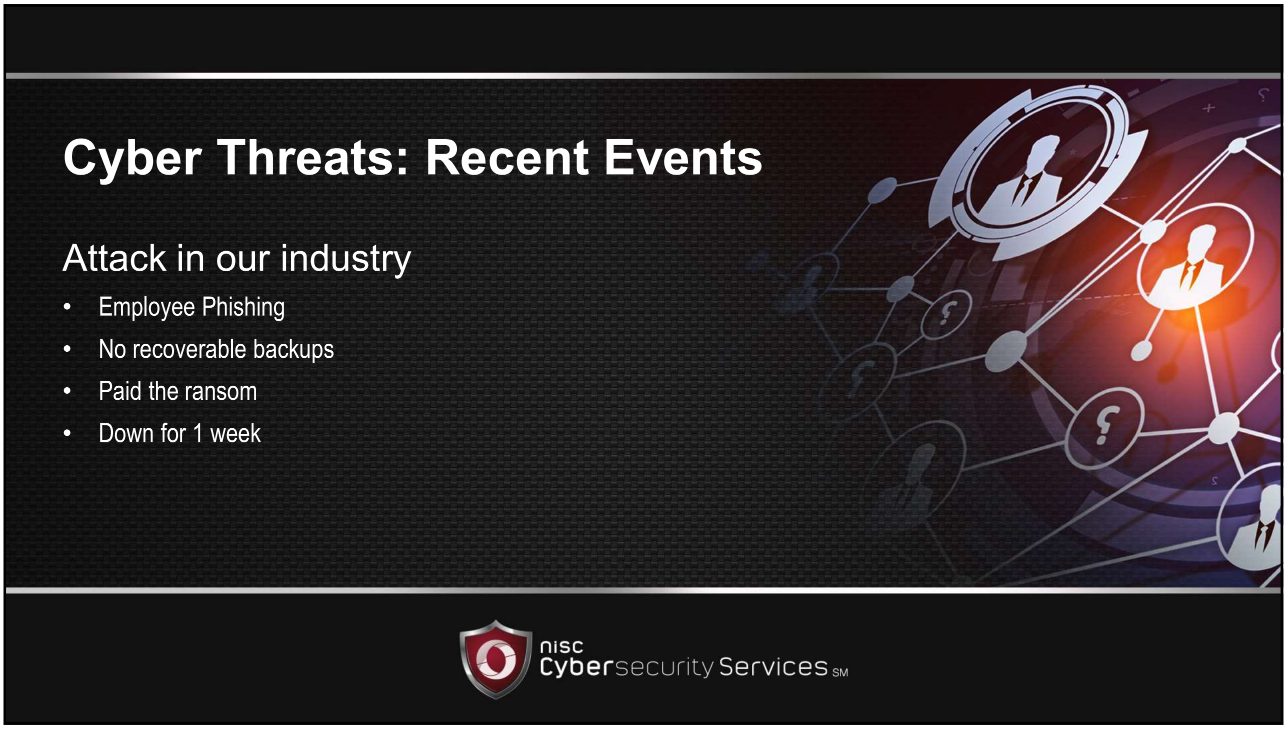
Cyber Threats: Recent Events

Attack in our industry

- Employee Phishing - Admin user
- Encrypted Windows network
- Had backup to restore from backup
- Down for 5 days

nisc Cybersecurity Services SM

16



Cyber Threats: Recent Events

Attack in our industry

- Employee Phishing
- No recoverable backups
- Paid the ransom
- Down for 1 week

nisc Cybersecurity Services SM

17

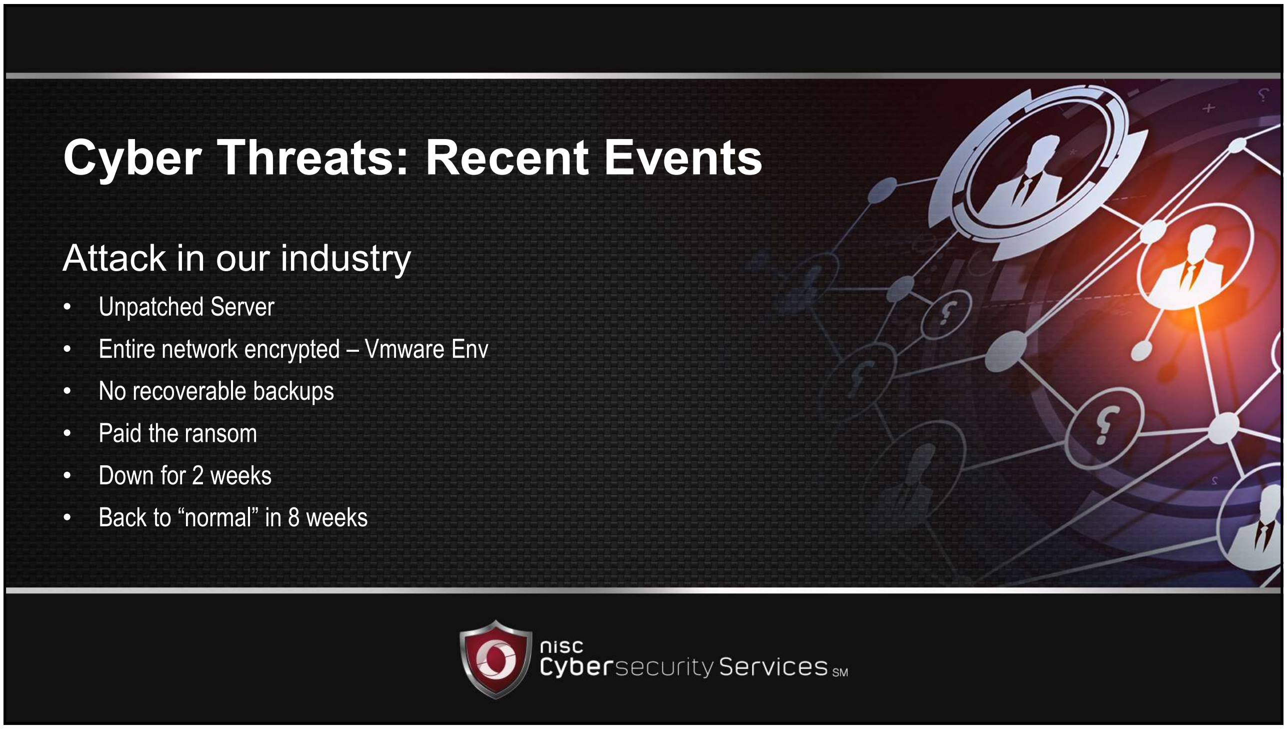
Cyber Threats: Recent Events

Attack in our Industry

- Remote access
- Vmware infrastructure encrypted
- Recoverable backups
- Did not pay the ransom
- Down for 24 hours
- Back to normal in 2 weeks

nisc Cybersecurity Services SM

18



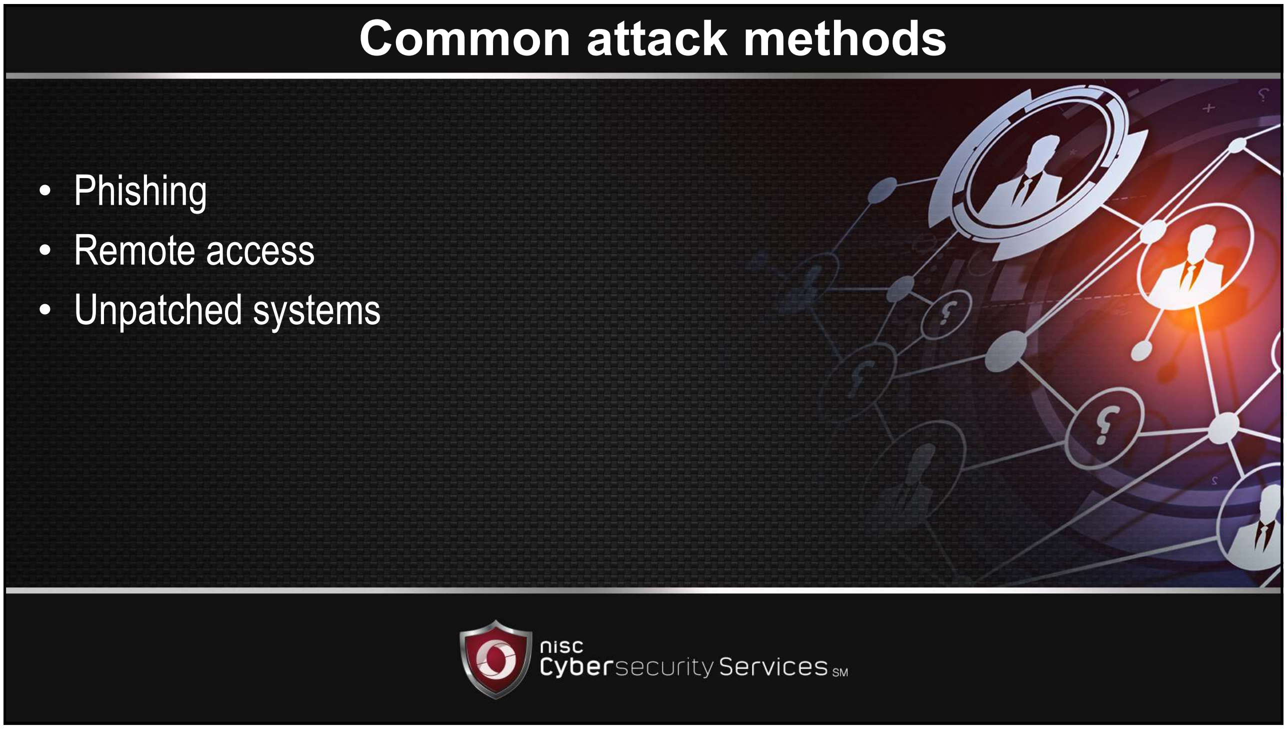
Cyber Threats: Recent Events

Attack in our industry

- Unpatched Server
- Entire network encrypted – Vmware Env
- No recoverable backups
- Paid the ransom
- Down for 2 weeks
- Back to “normal” in 8 weeks

nisc Cybersecurity Services SM

19



Common attack methods

- Phishing
- Remote access
- Unpatched systems

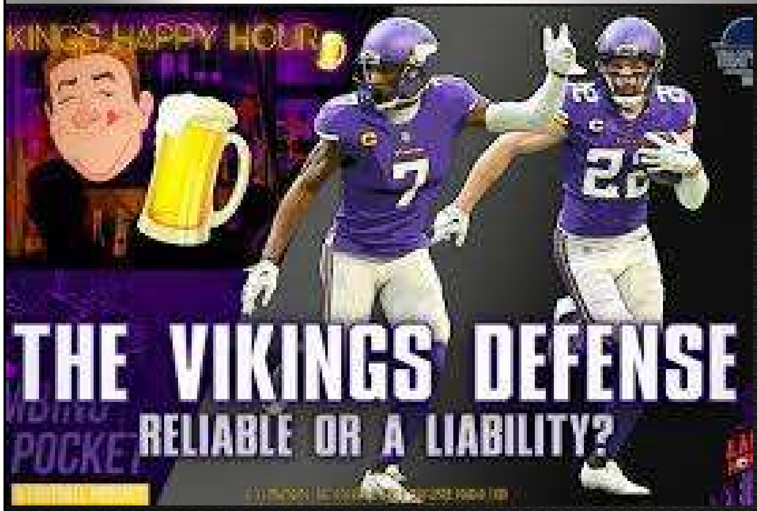
nisc Cybersecurity Services SM

20

How Do We Defend Against These Attacks?

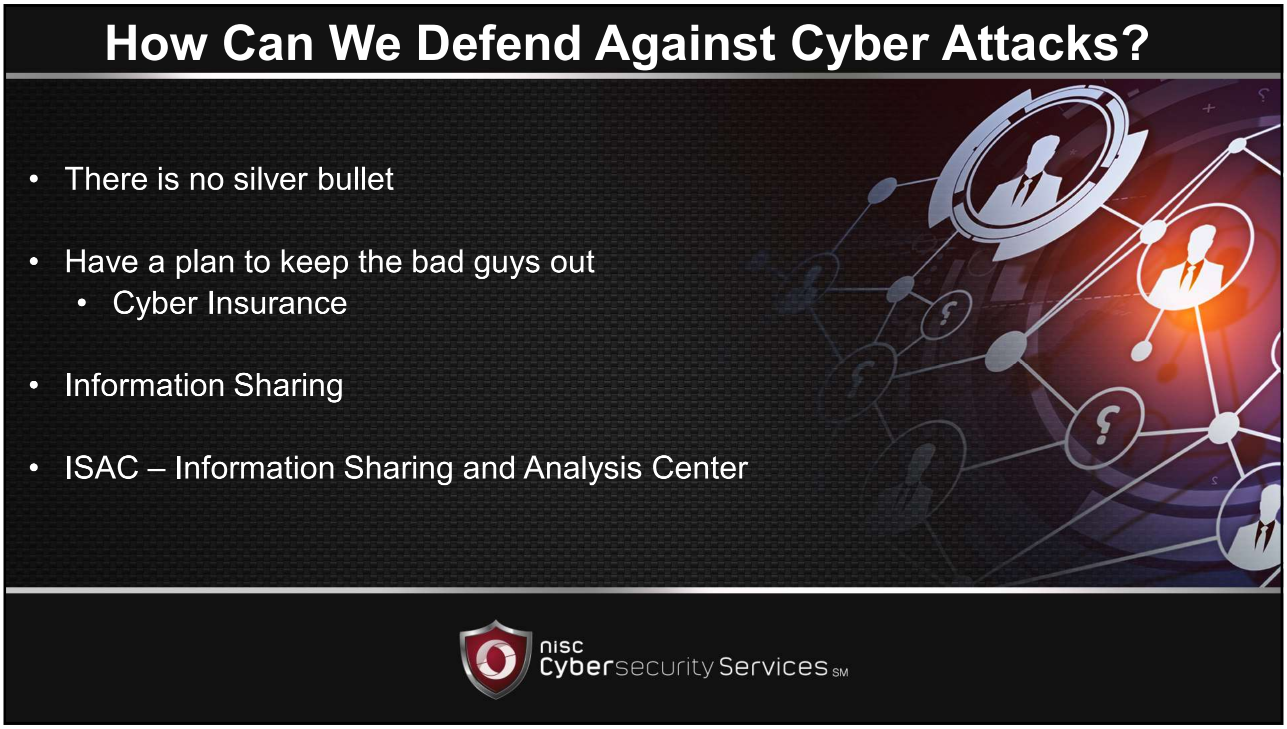
nisc Cybersecurity Services SM

21



nisc Cybersecurity Services SM

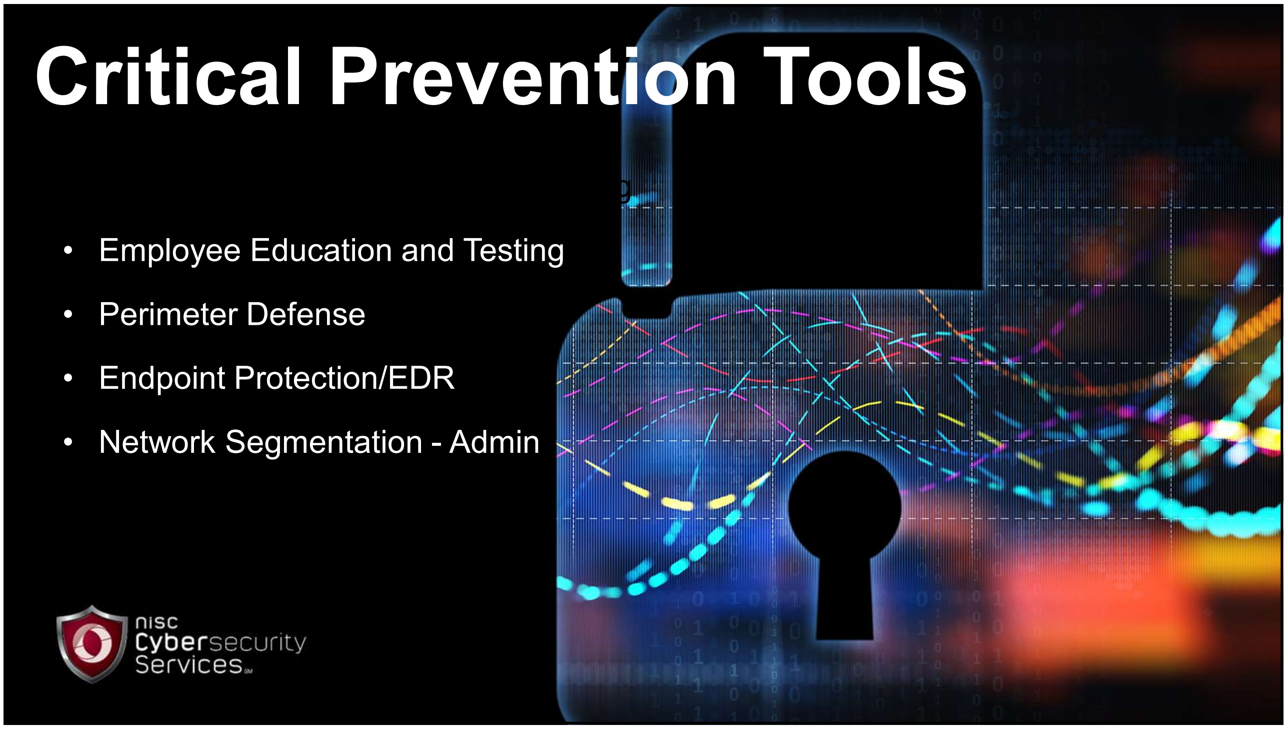
22



How Can We Defend Against Cyber Attacks?

- There is no silver bullet
- Have a plan to keep the bad guys out
  - Cyber Insurance
- Information Sharing
- ISAC – Information Sharing and Analysis Center

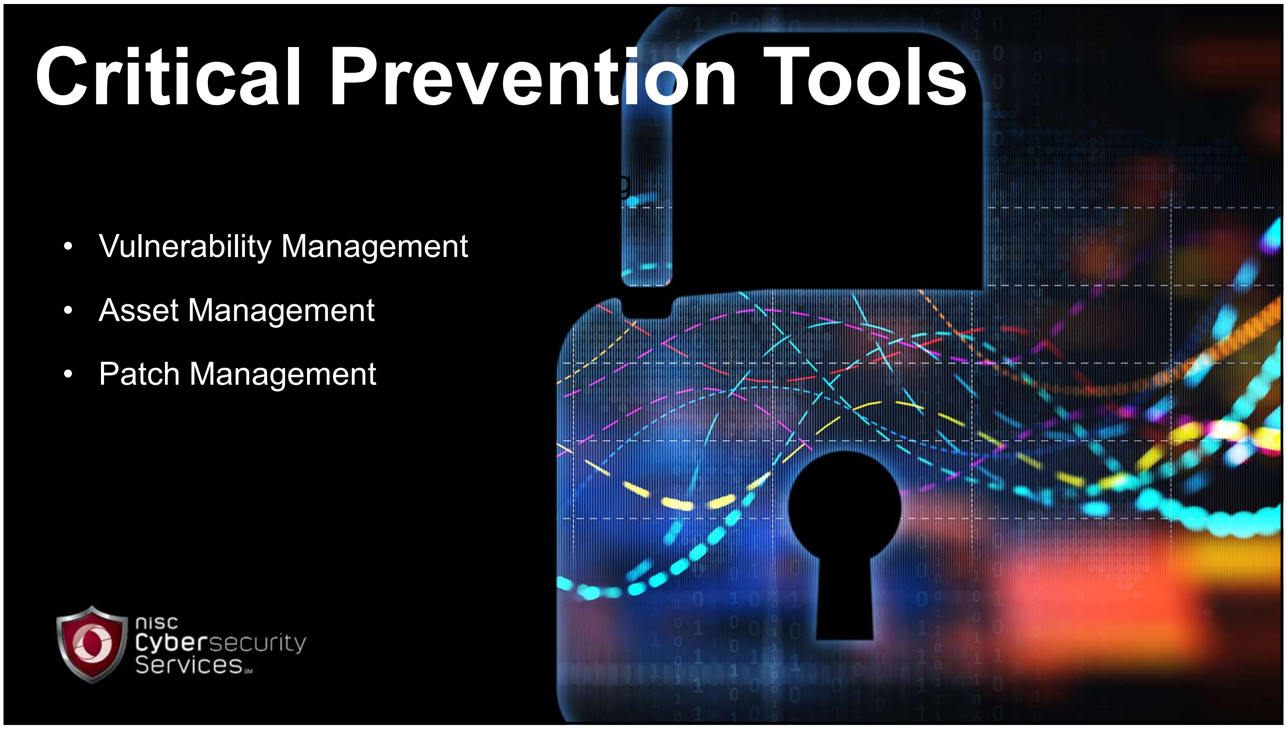
23



Critical Prevention Tools

- Employee Education and Testing
- Perimeter Defense
- Endpoint Protection/EDR
- Network Segmentation - Admin

24

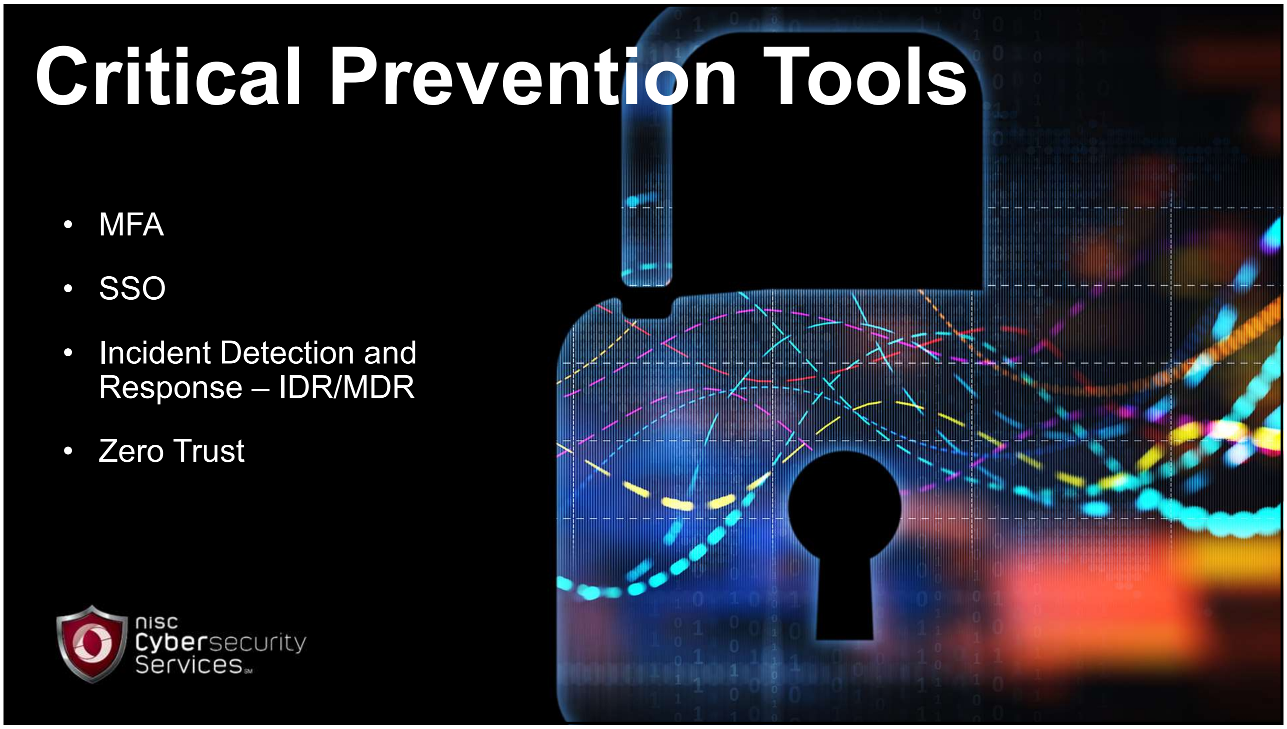


Critical Prevention Tools

- Vulnerability Management
- Asset Management
- Patch Management

nisc
Cybersecurity
Services

25

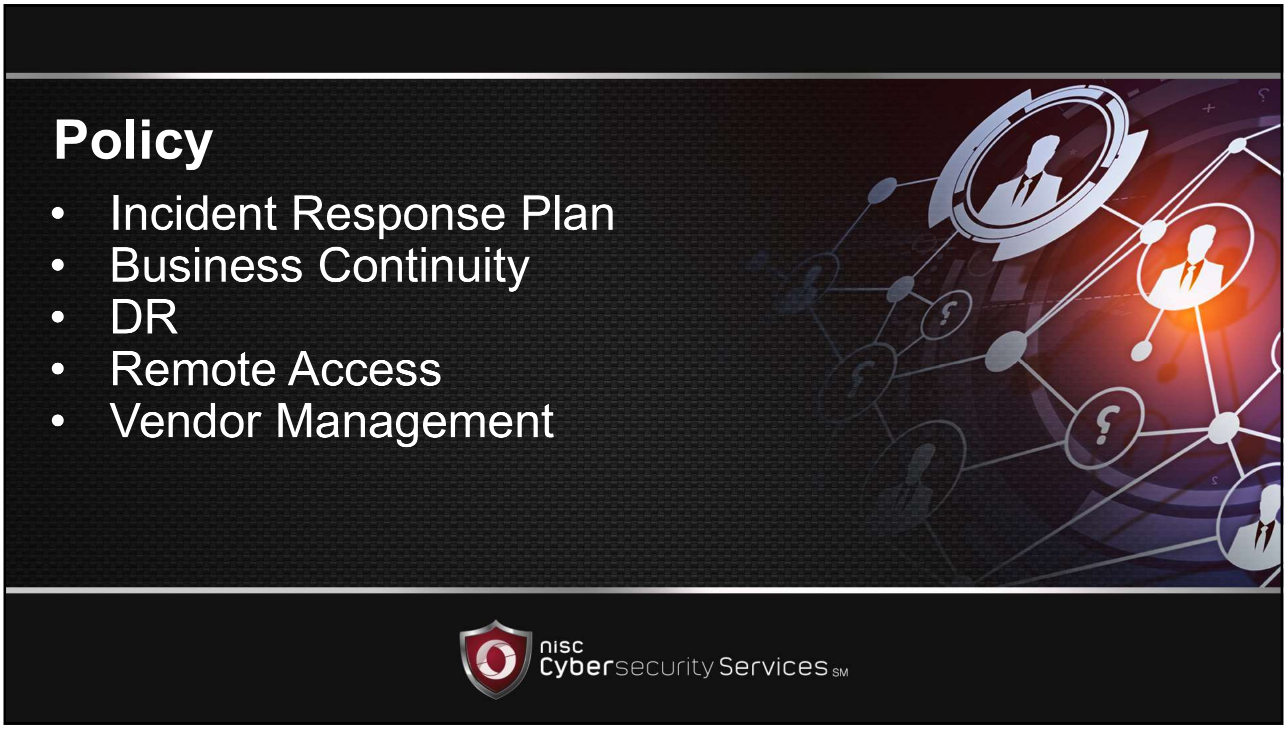


Critical Prevention Tools

- MFA
- SSO
- Incident Detection and Response – IDR/MDR
- Zero Trust

nisc
Cybersecurity
Services

26

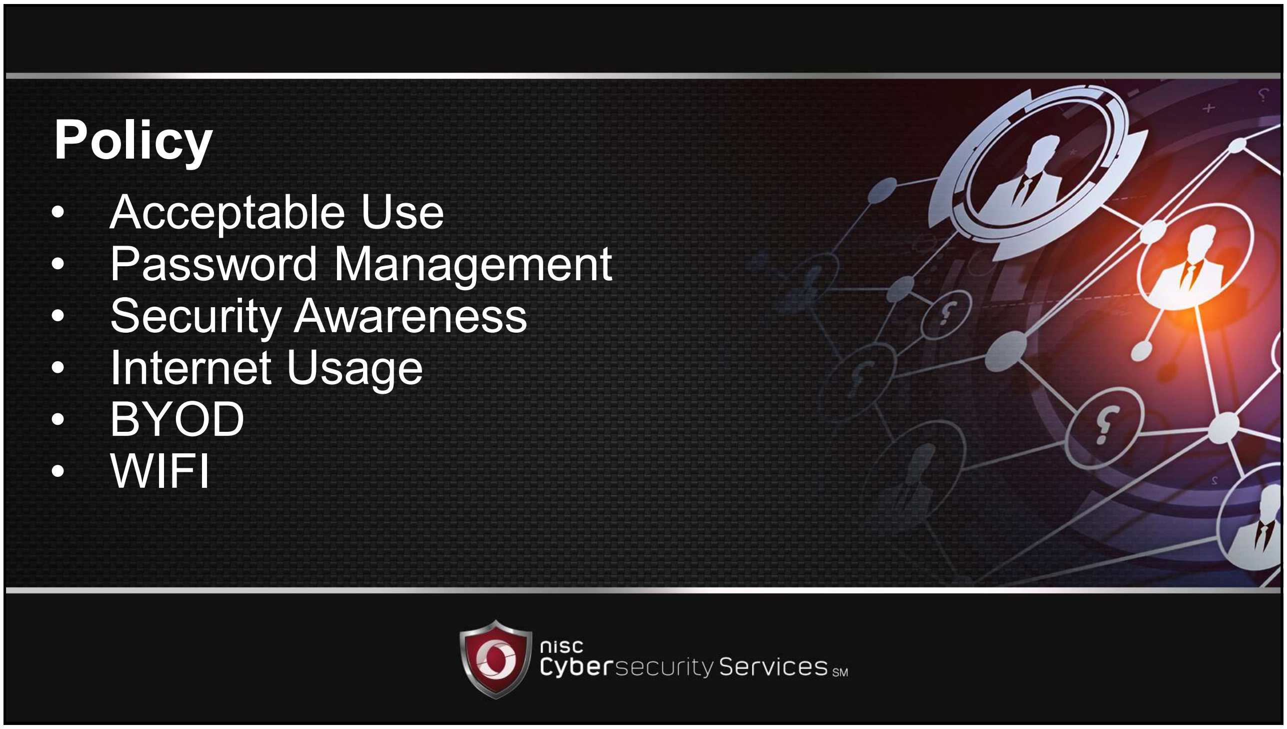


Policy

- Incident Response Plan
- Business Continuity
- DR
- Remote Access
- Vendor Management

nisc Cybersecurity Services SM

27

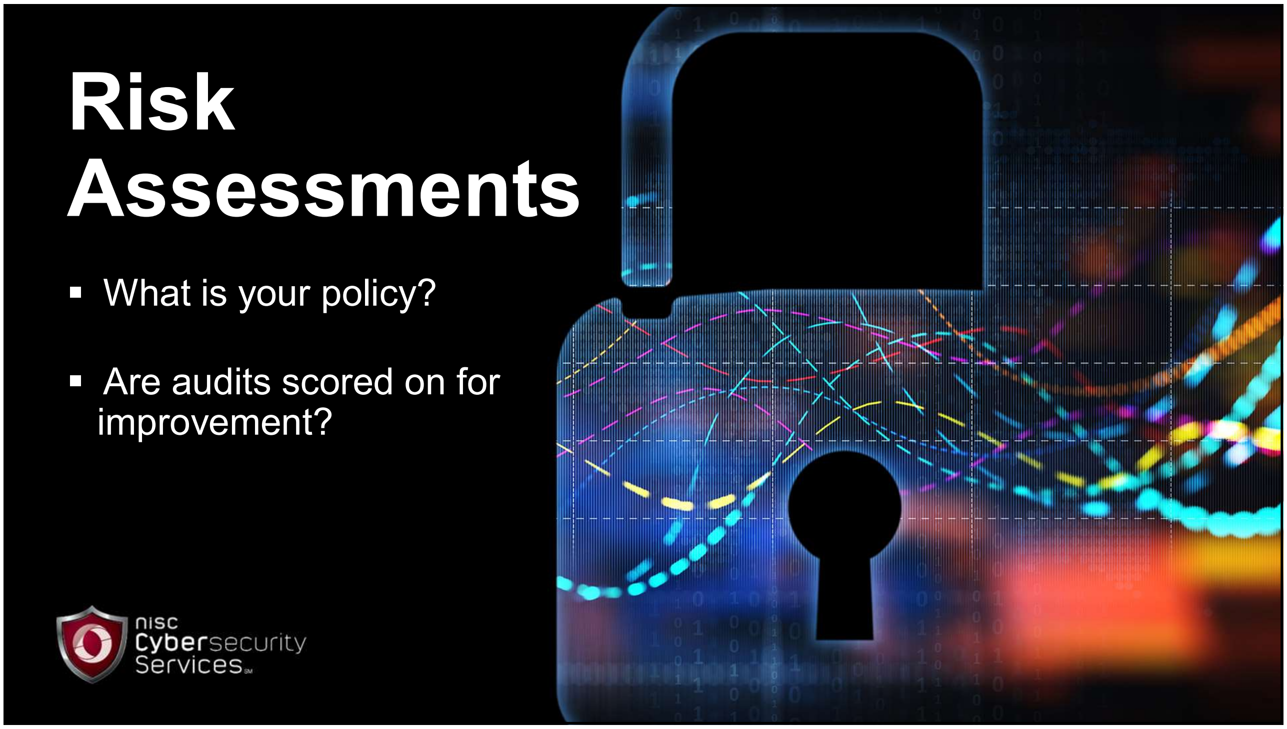


Policy

- Acceptable Use
- Password Management
- Security Awareness
- Internet Usage
- BYOD
- WIFI

nisc Cybersecurity Services SM

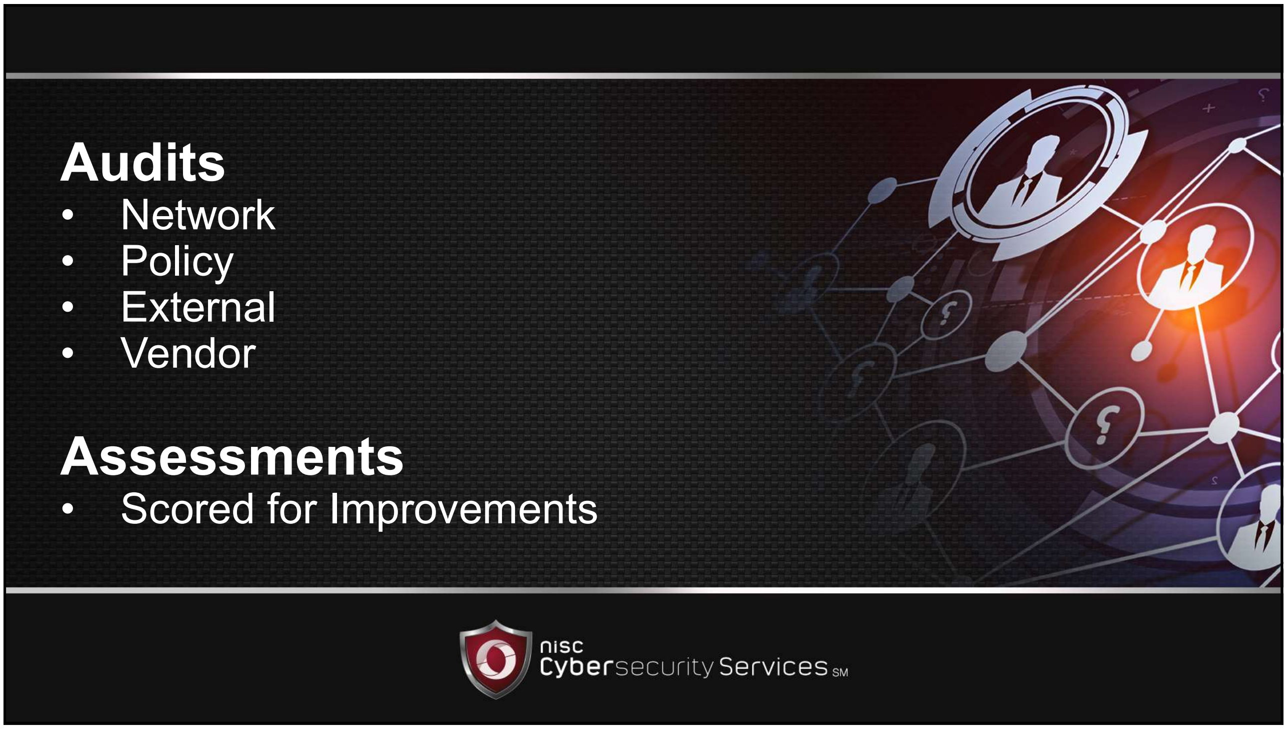
28



Risk Assessments

- What is your policy?
- Are audits scored on for improvement?

29



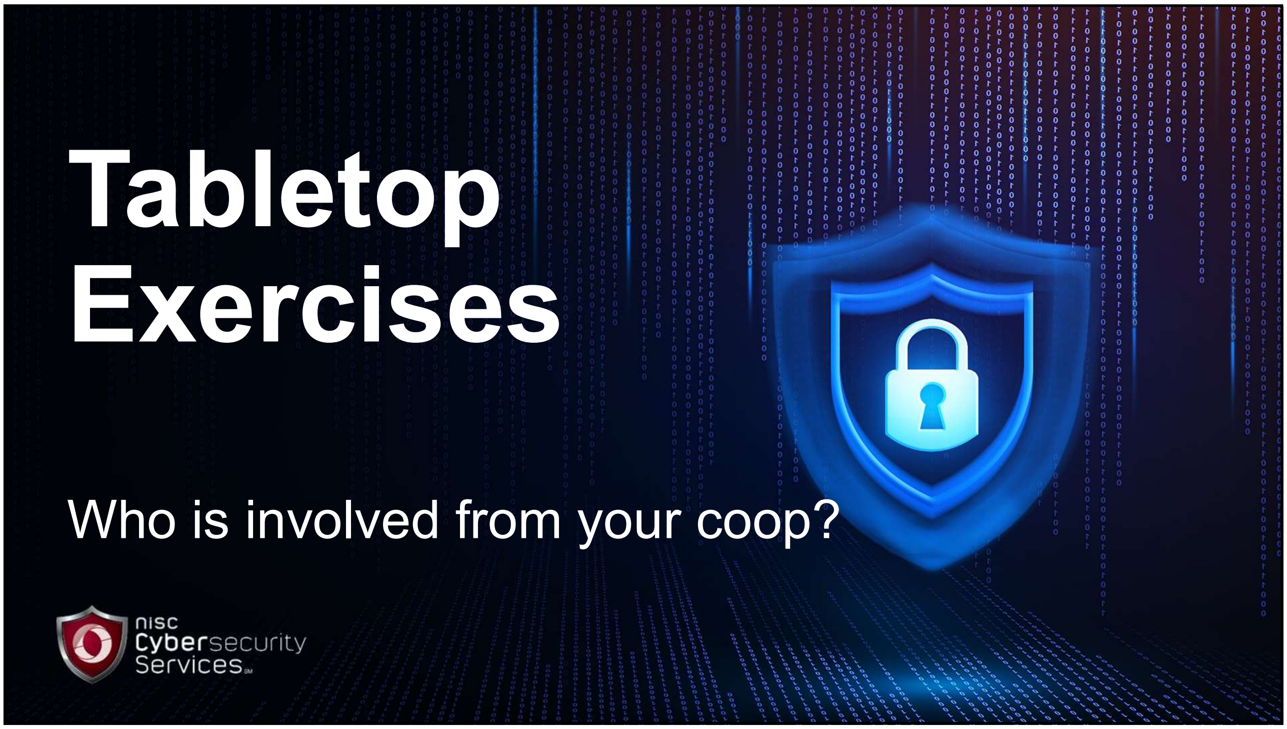
Audits

- Network
- Policy
- External
- Vendor

Assessments

- Scored for Improvements

30



Tabletop Exercises

Who is involved from your coop?

31

How Do You Recover from a Ransomware Incident?

- Define and put in place a strong **off-site, isolated backup strategy**
- Ensure your business is **uninterrupted** by the incident

32

THE STEEL CURTAIN

nisc Cybersecurity Services SM

33

nisc Cybersecurity Services SM

EDUCATION

ENDPOINT PROTECTION

INCIDENT DETECTION & RESPONSE

PERIMETER DEFENSE

VULNERABILITY MANAGEMENT

PATCH MANAGEMENT & AUTOMATION

BACKUP MANAGEMENT

IDENTITY AND ACCESS MANAGEMENT

nisc

34

nisc
Cybersecurity Services℠

Questions?

nisc

35

nisc
Cybersecurity Services℠

Thank You

nisc

36