Cybersecurity and Business

DS24
DataSure Twenty Four

www.datasure24.com | 716.600.DS24

Why are we here?

- Cybersecurity has become a critical part of most organizations

Why Cybersecurity is important

- Regulations
- Business Risks
- Employee Peace of Mind

Type of Threats

- Ransomware
- Data Theft
- Fraud
- Denial of Service
- Malware

Ransomware Methods

- Attackers exploit people or systems
  - Phishing
  - Direct Attacks
- Ransomware is installed
  - Encrypts files
  - Installs additional Malware
  - Attacks other systems on the network
- Ransomware is activated
  - Require payment to decrypt data

Ransomware Responses

- Technology based protections
- Security awareness training
- Pay Ransom

Threat Weaknesses

- Lack of IT/Security Personnel
- Cybersecurity Funding
- PII High Value Targets

2019 WILL BE THE YEAR
OF RANSOMWARE RISING

A new business will fall victim to ransomware every 14 seconds in 2019 – and every 11 seconds by 2021, according to Cybersecurity Ventures predictions.

ADDITIVE

ALWAYS
“EVOLVING”

NEVER
ENDING

CAT &
MOUSE

“SHOW ME
THE MONEY!”

Cyberthieves Are looking for

- Compromising emails
- Customer financial information
- Employee personal information
- Federal tax employer identification numbers
- Medical records
- Passwords
- Trade secrets
- W2s and tax data

It’s likely that cyberthieves are Marketing your company data on the dark web right now

- Blogs
- Bulletin boards
- Forums and chat rooms
- Malwares samples
- Peer-to-peer sharing networks
- Social media feeds
- Web pages
- Web services and servers

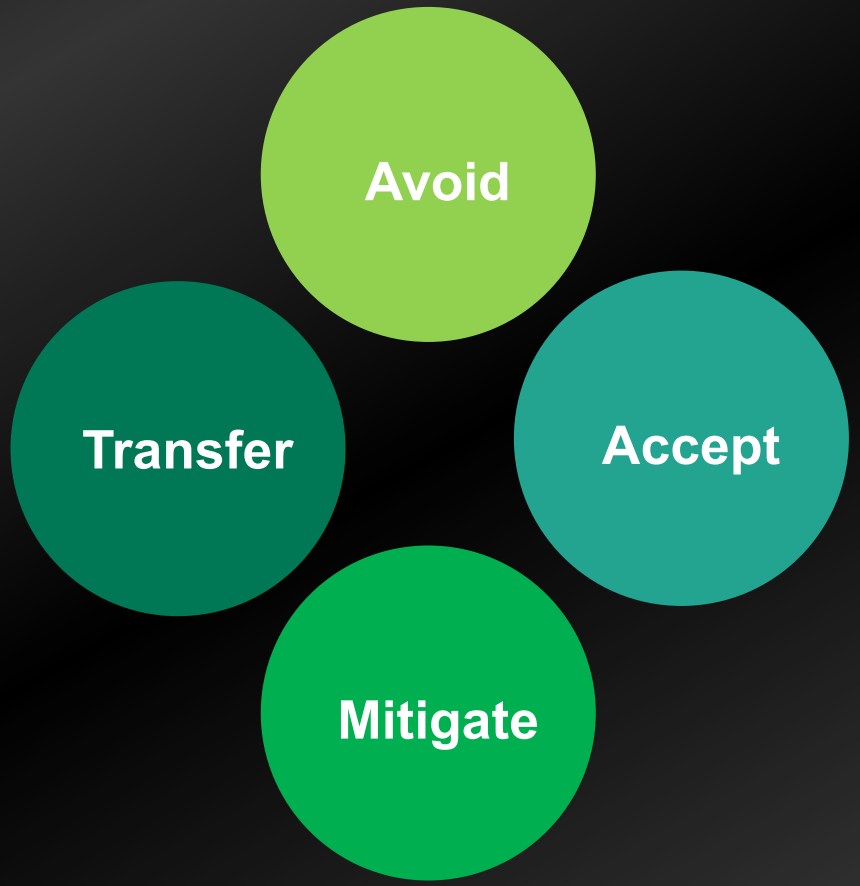
Methods of Protection

- Proactive
  - Training
  - Vulnerability Remediations
  - Hardening
  - Monitoring
- Reactive
  - Monitoring
  - Incident Response

Incident Response

- An incident is an event that could lead to loss of, or disruption to, an organization's operations, services or functions.

Cyber Risk Responses



Cyber Insurance

- Covers losses related to an incident
  - Actual losses
  - Theft
  - Ransom
  - Incident Response
  - Reputation
  - Remediation
- Failure to safeguard data

Next steps

- Questions to ask
  - Explain current cybersecurity program
  - What frameworks are used
  - What is cybersecurity budget
  - Existing/last security assessment
  - Existing remediation items
  - Third-party security assessments