

IS YOUR
BUSINESS AS
SAFE AS
YOU THINK?



JAMES SANFORD - TEAMSPRING

COULD YOU BE AT RISK?

Hackers know that most smaller organizations are not prepared for network security breaches, making them popular targets for cyberattacks.¹

¹15 Small Business Cyber Security Statistics That You Need to Know, thestatstore.com, December 2020



PRESENTATION OVERVIEW

- ▶ Cyber Security Overview
 - ▶ Prevention * Detection * Response
- ▶ Before the Boom – Not if but when
 - ▶ Employee Education
 - ▶ Technology Prevention
 - ▶ Cyber Insurance & Planning
- ▶ After the Boom – Recovery



YOU HAVE WHAT THEY WANT

Your business is an attractive target because you have items that cybercriminals want, but you may lack the security infrastructure of larger businesses.²

²As Cyberattacks Become More Prevalent, Here's Why Your Small Business is at Risk. securitymagazine.com, February 2020

PERSONAL DATA

Small companies collect data, such as medical records, credit card information, social security numbers, bank account credentials or proprietary business information, that is easy to offload for a profit on the dark web.

CONNECTIONS

A smaller vendor led to the Target breach, which resulted in 40 million stolen credit and debit cards. Hackers accessed the retail giant's system through a subcontractor that provided refrigeration and HVAC systems.

POOR MONITORING

An organization succumbed to a ransomware assault and paid millions for the decoding key to regain their network access. However, they failed to identify how it happened. As a result, they were retargeted by the same group within two weeks.

COLD CASH

Money is a powerful motive, which is why ransomware has become such a popular method of attack. The average cost of a ransomware attack on a business today exceeds \$133,000.

- ▶ Prevention
- ▶ Detection
- ▶ Response

CYBERSECURITY OVERVIEW

FIREWALLS & ANTIVIRUS SOFTWARE AREN'T ENOUGH

Vulnerabilities can be managed only if they have been discovered and identified.³ Vulnerability scans are typically required quarterly or monthly, depending on the cybersecurity framework being followed.

³Costs and Consequences of Gaps in Vulnerability Response study, Ponemon Institute, February 2020



- ▶ Employee Education -
 - ▶ Awareness Training
- ▶ Technology Solutions
 - ▶ Prevention
 - ▶ Layered approach – Email-> Firewall-> AV-> Breach Detection-> SOC
 - ▶ Team Training
- ▶ Cyber Insurance
 - ▶ Check your policy
 - ▶ Answer the questions properly
 - ▶ What does it pay for?

BEFORE IT GOES WRONG

BUSINESS CONTINUITY PLANNING (BC)

Contact Cyber Insurance

- Preserve the evidence – Don't just start recovery
- Notification / PR (talking to the public) / Compliance (Hipaa?)
- Law enforcement / Insurance appointed attorney / Your I.T.

Data Recovery

- Onsite / Offsite and TEST, TEST, TEST

Postmortem to review

THE AFTERMATH - RECOVERY

RECOVERY POINT OBJECTIVE (RPO)

RECOVERY TIME OBJECTIVE (RTO)

Disaster hits



Technology Review

- Who is responsible for this in your organization
- Are all your tools up to date?
- Where is there room for improvement?

Struggles

- Budget / Team Members / Tech Skills

Thankful

- It hasn't happened to you!

WHAT'S
NEXT!



James Sanford

- James@teamspring.us
- 770-614-9495

www.teamspring.us/

Thank You!!!

CALL ME!

Decorative white lines consisting of several parallel lines of varying lengths and orientations, located in the bottom right corner of the slide.