THE IMPORTANCE OF LAYERED CYBERSECURITY

IN THE REMOTE WORK LANDSCAPE

WHAT IS CYBERCRIME?

PERPETRATORS AND ATTACKS

COMMON MISCONCEPTIONS

DON'T BE THE VICTIM

REMOTE WORK + CYBERSECURITY

WHAT IS CYBERCRIME?

- Cybercrime is a broad range of malicious activity from cyberbullying to worms/viruses, but it also includes:
- Illicit, illegal online markets
- Trade secret, IP theft
- Crimeware, CaaS (Crimeware-as-a-service)
- Ransomware

WHY SHOULD I CARE ABOUT CYBERCRIME?

Victims of cyberattacks experience a variety of losses:



CUSTOMER PROTECTION



CAREER DAMAGE



COMPANY REPUTATION



FINANCIAL COST



PRODUCT PROTECTION



PASSWORD ATTACKS



TROJAN HORSES



SPYWARE & EAVESDROPPING

DIRECT ASSAULTS



SMB

SNEAK ATTACKS



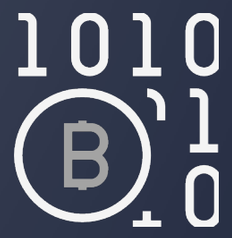
MALWARE, WORMS, AND VIRUSES



DDOS ATTACKS



PHISHING



RANSOMWARE

HOW MUCH IS BUSINESS DATA WORTH TO BAD ACTORS?

6 billion digital records exposed 2018
43% of all breaches involved SMB victims

CREDIT CARD INFO
$2-$5 PER RECORD

CUSTOMER PII
$20-$450 PER RECORD

EMPLOYEE PII
$20-$450 PER RECORD

MEDICAL RECORDS
$20-$50 PER RECORD

PROPRIETARY INFO
COMPETITIVE VALUE

SALES/FINANCIAL INFO
COMPETITIVE VALUE

Source: Per the Verizon Data Breach Investigation Report
Estimated data values from Sociable

WHAT IS THE IMPACT OF DOWNTIME?

WHEN IT COMES TO RANSOMWARE ATTACKS, **MSPs REPORT THE COST OF DOWNTIME IS**

23X

GREATER THAN THE RANSOM REQUESTED

DATA'S RESALE VALUE DOESN'T MATTER WHEN IT COMES TO RANSOMWARE

Ransomware attackers don't need to be able to monetize stolen data, that just need to be victimized business to require their data enough to pay to get it back.

58% of businesses who paid a ransom in the last 12 months, did so because the cost of the ransom was less than the cost of lost productivity from downtime due to the attack.

Source: Datto 2019 State of the Channel Ransomware Report

INDUSTRIES AFFECTED

Industries most targeted by ransomware:

32%
OF MSPS REPORT
CONSTRUCTION & MANUFACTURING
MOST TARGETED BY RANSOMWARE

- **31%** Professional Services
- **23%** Healthcare
- **20%** Financial/Insurance
- **18%** Legal
- **15%** Retail
- **12%** Real Estate
- **9%** Architecture/Design
- **9%** Government
- **8%** Education
- **7%** Consumer Products
- **5%** Travel/Transportation
- **6%** Media/Entertainment
- **4%** High Technology
- **4%** Energy/Utilities
- **2%** Telecom
- **11%** Other/None

Source: Datto 2019 State of the Channel Ransomware Report

COMMON MISCONCEPTIONS

Misconceptions are reflected in what SMBs are saying:

“ **WE HAVE ANTIVIRUS SOFTWARE.** ”

“ **OUR DATA IS IN THE CLOUD.** (SO IT’S SAFE RIGHT?) ”



“ **WE’RE TOO SMALL TO BE TARGETED.** ”

“ **AN ATTACK/BREACH WON’T HAPPEN TO US.** ”

“ **WE DON’T HAVE ANYTHING HACKERS WANT.** ”

COMMON MISCONCEPTIONS

47% of data loss was due to end users deleting information and 17% was due to users overwriting data.



“I’M JUST NOT THAT WORRIED ABOUT BEING HACKED.”

- SERVER ISSUES
- HUMAN USER ERROR
- POWER OUTAGES
- UNEXPECTED UPDATES
- SEVERE WEATHER
- FIRE DAMAGE

Source: CIO.com

COMMON MISCONCEPTIONS

Many SMBs are unaware of the dangers.

"...a data breach could well be fatal and end an SMB's business, while others remain unaware of the catastrophic potential, according to a new survey on cyberattacks and their impact on American businesses with employees numbering from 1-9 up to 200-250 per organization."

Roger Aitken, Forbes

Source: Forbes, Cybercrime & Hackers 'More Devastating' To SMB's Than Fire, Flood & Transit Strike Combined

DON'T BE A VICTIM

Modern companies need to become digital fortresses
With multiple layers of proactive protection that serve to monitor, detect, alert, and prevent the onslaught of cyberattacks.

- **IDENTITY PROTECTION & ACCESS MANAGEMENT**
- **REMOTE MONITORING AND SOC**
- **BACKUP AND DISASTER RECOVERY**
- **EMAIL SECURITY**
- **WEB AND NETWORK SECURITY**
- **END USER TRAINING**
- **ENDPOINT SECURITY**
- **MOBILE SECURITY**
- **DATA PROTECTION**

HOW TO

INSTANTLY ENHANCE YOUR ONLINE SECURITY



1

SET UP MULTI-FACTOR AUTHENTICATION

Bad actors are less likely to gain access to your company's resources, even if credentials become compromised.

2

BACK UP YOUR DATA REGULARLY

You can rest easy knowing that in the case of a cyber attack or disaster, your important files still exist somewhere.

3

USE A PASSWORD MANAGER

Password managers allow you to generate and save strong passwords, making it less likely for hackers to gain access.

COVID-19: ALARMING INCREASE IN CYBERCRIME



The FBI reported in August 2020 that cyberattack complaints are up by **400%!**



Microsoft reports that pandemic-themed phishing and social engineering attacks have jumped by **10,000 a day.**



Cybersecurity experts report that ransomware attacks are up by **800%.**

Source: MonsterCloud, Top Cyber Security Experts Report: 4,000 Cyber Attacks a Day Since COVID-19 Pandemic

REMOTE WORK & CYBERSECURITY

36% of organizations have dealt with a security incident due to an unsecured remote worker.

With the rise in remote work, IT security focus has shifted from the perimeter, network, and firewalls to endpoints, end users, and email as the first line of remote defense.



ENDPOINTS

64% of SMBs experienced one or more endpoint attacks that successfully compromised data in 2018.



EMAIL

65% of organizations in the United States experienced a successful phishing attack in 2019.



END USERS

55% of organizations don't provide any sort of email security training on a frequent basis.

Sources: OpenVPN, Ponemon Institute, HIPAA Journal, Mimecast

MANAGED SECURITY

SUMMARY

Today’s cybercriminals have adopted automation, which in turn has enabled them to cost effectively go after the SMB market. For partners to protect their clients more effectively and efficiently, there is a greater need to outsource advanced security to industry experts. Outsourcing their security operations enables partners to provide 24x7 security monitoring and incident response to protect SMB clients from today's advanced threats.

BENEFITS

- Provides a comprehensive view into the threat landscape across client base
- Helps to quickly identify threats to enable quick resolution
- Robust reporting helps convey value to end users

SOLUTION

COUNTYMICRO
YOUR TRUSTED IT SOLUTIONS PARTNER

COUNTYMICRO

YOUR TRUSTED IT SOLUTIONS PARTNER

HELLO@COUNTYMICRO.COM

(207) 521-9190

WWW.COUNTYMICRO.COM