Nationwide®
is on your side

USHCC
UNITED STATES HISPANIC CHAMBER OF COMMERCE

# *Cyber Security Solutions*

## How to help protect your small business

**Catherine Rudow & Abhay Joshi**
July 2020

**Catherine Rudow**
Vice President, Cyber Insurance

Catherine Rudow is Vice President of Cyber Insurance for Nationwide. With over 25 years' experience in the (re)insurance sector, she is responsible for developing and expanding the Cyber product expertise across Nationwide. Prior to her current role, Catherine served at PartnerRe overseeing underwriting for and managing PartnerRe's North American cyber insurance portfolio. As an expert in cyber insurance risk, she speaks frequently at national and international conferences on a broad range of cyber topics. Her background also includes Tech E&O, professional liability and casualty lines of business.

Catherine has a Bachelor of Science and Bachelor of Commerce from Concordia University, Montreal and earned her Master of Business Administration at Yale University.

**Abhay Joshi**
Consultant, Information Risk Management

Abhay Joshi is an Information Technology Risk Management Professional at Nationwide, one of the largest insurance and financial services companies in the world.

Abhay is a Certified Information Systems Security Professional (CISSP). He has more than 20 years of experience in Information Technology, including six years of consulting on numerous Cyber Security and IT Risk Management initiatives across multiple security domains and technologies.

In his current role, he provides security consulting to application teams to ensure that enterprise standards are being adopted and risk is managed at an acceptable level. In addition, he assists teams in meeting their regulatory, audit and compliance requirements.

# Disclaimer

*The information used to create this presentation deck was obtained from sources believed to be reliable. Nationwide Mutual Insurance Company and its employees make no guarantee of results and assume no liability in connection with any information provided. It is the user's responsibility to confirm compliance with any applicable local, state or federal regulations. Information obtained from or via Nationwide Mutual Insurance Company should not be used as the basis for legal advice or guidance. Nationwide, Nationwide is on your side, and the Nationwide N and Eagle are service marks of Nationwide Mutual Insurance Company.*

*© 2020 Nationwide*

## POLL QUESTION #1

Most small companies are “too small” to be targeted by cyber criminals.

a) **True**

b) **False**

c) **Don’t know**

# Small businesses don’t always take cyber threats seriously

- Don’t focus on IT because they don’t think it will happen to them.
- 54% of SMBs Believe Their Companies are “Too Small” to Be Ransomware Targets per The Keeper Security/Ponemon Institute study
- Nationwide’s 2018 Business Owner’s survey showed that 34% businesses don’t have a dedicated employee or vendor for cybersecurity because they don’t think their business will be the target of cyber attacks.
- Criminals use automation (vulnerability scanners and bots) to quickly find potential targets, so even small organizations are “on the radar.”

# In fact, small businesses are tempting targets

- So many of them… a big pool of targets!
- Path of least resistance: less sophisticated systems
- Easier to breach
  - Less employee training. Nationwide’s 2019 business owners survey indicated that 50% of businesses with 11-50 employees train their employees sporadically or not at all.
  - Less monitoring
  - Less patching
- Less resources
  - Juniper Research’s 2018 study shows that small businesses invest less than $500/year for consumer-grade cyber security products
  - Nationwide’s 2018 Business Owner’s survey showed that 33% of business owners cite cost as the reason they don’t have a dedicated employee or vendor

# Cyber Risk Exposure for Small businesses

- Nationwide’s 2019 Business Owners survey indicated that 86% of business owners believe that digital risk will continue to grow – They’re right!
- According to the 2018 NetDiligence Claims Study, the percentage of claims emanating from the small business segment continues to increase, and in 2017 accounted for 61% of claims.
- FireEye found that over 77% of all cyber crimes target small and midsize enterprises (SMEs).
- Unfortunately, Hiscox 2018 Small Business Cyber Risk Report found that 7 out of 10 businesses are unprepared to deal with a cyber attack.

# Cyberattack Costs for small businesses

- 83% of SMBs Lack the Funds to Deal with the Repercussions of a Cyber Attack*
- Nationwide’s 2018 Survey of business owners found that one third of cyber attacks cost business owners $50,000 or more to recover from, and nearly half (45%) said they needed more than three months to resume normalcy.
- Costs of a cyberattack can include notification, paying extortion, forensics to discover and rectify problem, required upgrades, business interruption from down time, fines and penalties, lawsuits, lost reputation, etc.

*InsuranceBee’s Cyber Survey of 1300 SMB owners

# How do attackers gain access?

- Social Engineering, primarily Phishing
- Remote Desktop Protocol
- Unpatched Systems
- Compromised Passwords
- Infected Websites
- Managed Service Providers

# Main Cyber Losses for Small Businesses

- Ransomware
- Data breach
- Business interruption from a cyber event
- Reputational damage
  - Nationwide's 2019 Small Business Owners Survey found that for 45% of business owners, protecting their company's reputation is among a top reason for considering the purchase of a cyber risk insurance policy
- Business email compromise aka payment instruction fraud

# Ransomware Explained

- Ransomware attack occurs when the malware/ransomware accesses the computer system and proceeds to encrypt all files and data. To get the encryption key to unlock the files requires a ransom payment in cryptocurrency, often bitcoin.
- Ransomware can dwell on a system for some time before it is triggered.
- It is quite easy, lucrative, and any organization large or small, in any business sector, can be a victim. Behind the scenes, the criminals are organized, even selling RaaS (Ransomware as a Service), so criminals don’t even have to be very tech savvy to get in on the game!
- Cybersecurity Venture predicts that ransomware damage will exceed $11 billion in 2019.

# Ransomware Trends

- Complexity and sophistication of attacks are increasing
- Ransomware combined with data breach
  - Attackers are exfiltrating files/data before encryption, and threatening to release information if their demands are not met, doubling their leverage in negotiations.
- Demands are going up
  - Coveware noted that ransomware payments have risen significantly since mid-2018 (average less than $25K) to an average of $111.6K in first quarter 2020. That doesn’t include all other expenses associated with a ransomware attack, such as forensics and business interruption.

# Data Breach Explained

- According to the 2019 Verizon Data Breach Investigations Report 43% of data breaches involved small business victims.
- Types of Data
  - PII, PHI, Financial Information & Credit Card Information (regulated)
  - Intellectual Property/Trade Secrets (not regulated)
- Regulation – Requirements to protect and notify
  - Federal (e.g. HIPAA for healthcare, GLBA for Financial Institutions, etc.)
  - State (all states have laws, many of them vary in complexity)
  - PCI (for merchant banks that process credit card information)
- Responsibilities
  - Notification, credit monitoring
  - Forensics
  - Upgrade or replace systems
  - Third party liability
  - Fines and Penalties
- Reputational harm

# Business Interruption Explained

- Ransomware
- Denial of Service (DoS) Attack
  - When perpetrator overwhelms a website/network with traffic, causing the site to slow down or crash and making it unusable to legitimate users
- System Failure
  - When your network suffers an outage due to an operational/IT issue
- Third Party Dependency (Contingency Business Interruption)
  - When a supplier you depend on suffers a business outage, and it impacts your network/business income.

# Business email compromise (BEC) explained

- The FBI's Internet Crime Complaint Center (IC3) has reported 2019 losses for Business Email Compromise (BEC) and Email Account Compromise (EAC) at $1.7 billion.
- It all boils down to the victim sending money (or sensitive data) to the attacker's account!!
  - Social Engineering – more sophisticated
  - It's a scam.
  - Involves impersonation.
- Very common threat to law firms and real estate, but happens to all companies.  In current environment, healthcare under attack.
- COVID19 can make it easier to succeed – WFH has employees distracted and off guard

# Tips for enhancing cyber security Business Email Compromise (BEC)

- Employee Training!!!
- Use two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business it claims to be from.
  - Be alert to hyperlinks that may contain misspellings of the actual domain name.
  - Verify the email address used to send emails, especially when using a mobile or handheld device by ensuring the senders address email address appears to match who it is coming from.
  - Ensure the settings the employees' computer are enabled to allow full email extensions to be viewed.
- Have processes to check and authenticate payment info changes via multiple types of methods.
  - Require face-to-face meetings and/or direct phone calls when any changes to payment information are being detected.
- If you discover that you are the victim of a BEC scam, get in touch with your financial institution to request a recall of funds.
- The FBI also suggests to file a complaint regardless of the amount with www.ic3.gov or, for BEC/EAC victims, BEC.IC3.gov.

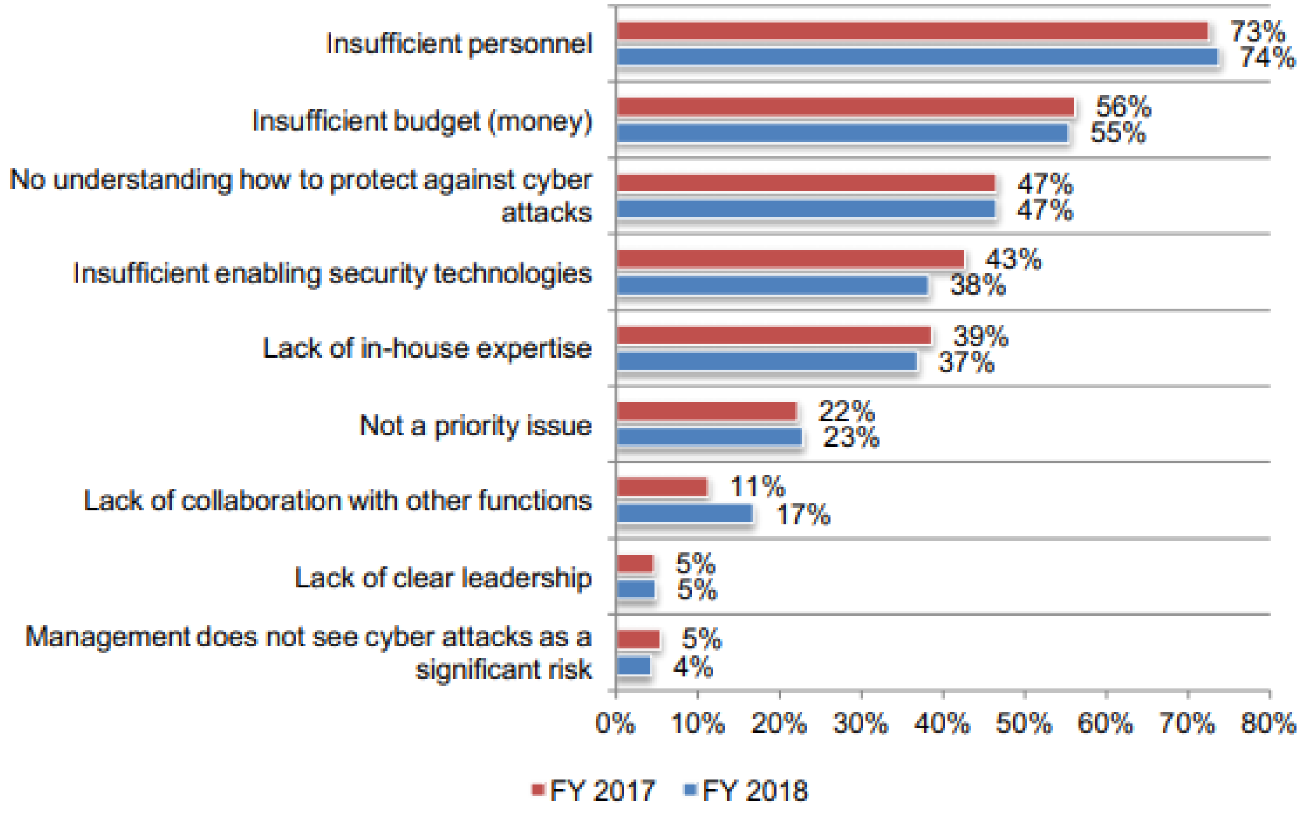
## POLL QUESTION #2

What challenges keep your IT security posture from being fully effective? Pick up to 3

a) **Insufficient personnel**
b) **Insufficient budget**
c) **No understanding how to protect**
d) **Insufficient enabling technologies**
e) **Lack of in-house expertise**
f) **Not a priority issue**
g) **Lack of collaboration with other functions**
h) **Lack of clear leadership**
i) **Management does not think cyber risk is significant**

# Ponemon/Keeper 2018 State of Cybersecurity in Small & Medium Size Business

**Figure 13. What challenges keep your IT security posture from being fully effective?**
Three choices allowed



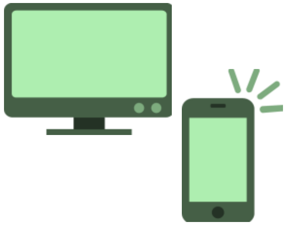
# Tips for enhancing cyber security

- Employee Training and Awareness
- Endpoint Security
- Network Security
- Identity and Access Management
- Email Security
- Scanning and Patching
- Back-up and Recovery Planning
- Incident Response Plan
- Managed Security Services
- Cyber Risk Insurance

# Tips for enhancing cyber security: Employee Training and Awareness

- Humans have become the primary attack surface for cyber criminals, so employee training is vital
- Employee Cyber Security Readiness Program should include:
  - ❑Communication of your information security policy
  - ❑Ongoing Security Education & Awareness Campaigns
  - ❑Focus on safe email, internet, and social media practices
  - ❑Training them to identify and report cybersecurity threats
  - ❑Conducting Internal Phishing Tests
- Human Resource Policies:
  - ❑Background checks on employees that will handle sensitive data
  - ❑Incorporate cyber security training into your onboarding program
  - ❑Revoke all access immediately after employee has left the company

# Tips for enhancing cyber security: Endpoint Security



- Enforce use of passwords to prevent unauthorized access
- Install anti-virus / anti-malware software
  - Run scans on an automated schedule
  - Keep software updated
- Email gateway to block phishing and social engineering attempts
- Web security policies to ensure safe browsing on the web
- Mobile Device Management (MDM) Solutions
  - Helps isolate company data
- Implement data loss prevention tools to identify and prevent data exfiltration
- Implement endpoint encryption to prevent data loss

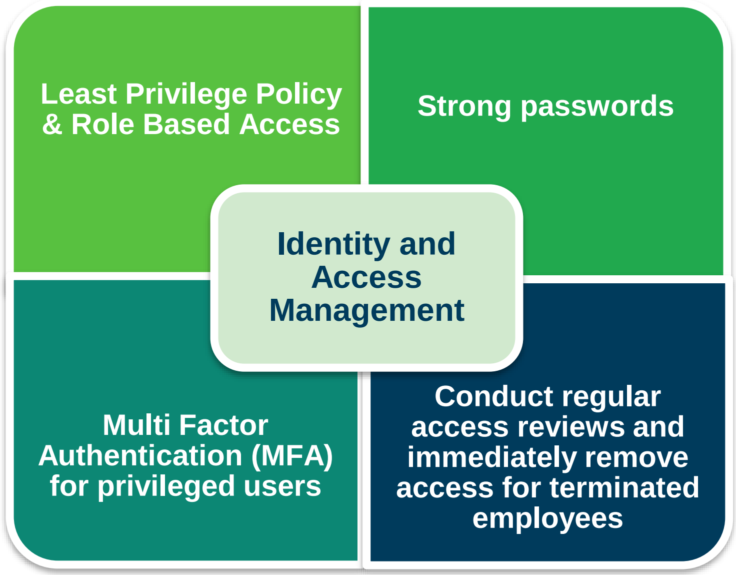
# Tips for enhancing cyber security: Network Security

- Implement firewalls to control access to your data - know who is on your network!
  - Monitor your network for intrusion
- Implement Virtual Private Network (VPN) to connect to your network remotely
- Disable or limit Remote Desktop Access to your network
- Protect your wireless network
  - Enforce passwords
  - Change default router passwords
  - Update router software/firmware
- Web security – protect your own web presence and brand reputation
  - Scanning and remediating vulnerabilities on website

# Tips for enhancing cyber security: Identity and Access Management

Identity management is a foundational security component:

- Implement Least Privilege Policy
- Implement Role Based Access
- Use strong, long, and unique passwords for all your accounts
- Implement Multi Factor Authentication (MFA) for Administrator access (privileged users)
- Conduct regular access reviews
- Remove access immediately for terminated employees


Least Privilege Policy & Role Based Access
Strong passwords
Identity and Access Management
Multi Factor Authentication (MFA) for privileged users
Conduct regular access reviews and immediately remove access for terminated employees

# Tips for enhancing cyber security: Email Security

Emails are often the threat vector for a security breach

- Train employees to protect against phishing, malware, ransomware threats
  - Check the email “from” field to validate the sender
  - Look closely at website addresses (URL) that are included in an email
  - DO NOT open any email attachments from unknown senders
  - DO NOT click embedded hyperlinks from unknown senders
  - DO NOT respond or reply to spam
- Implement an email security application that blocks incoming attacks and controls outbound messages to prevent the loss of sensitive data.
- Employees should not use company email for their personal email communication

# Tips for enhancing cyber security: Scanning and Patching

- Inventory your systems and supporting infrastructure (know what you have!)
- Develop a regular patching schedule
- Prioritize vulnerability remediation based on criticality and relevance
  - As an additional resource, please visit https://cve.mitre.org/
- Test thoroughly prior to deployment & have a back out plan

# Tips for enhancing cyber security: Backup and Recovery Planning

- Create a backup and recovery plan
  - Understand your critical assets
  - Document any external vendor dependencies
  - Ensure plan is accessible during a disaster event
  - Keep plans updated as your business evolves
- Regularly backup your critical data
  - Cadence should match your Recovery Time Objectives and Recovery Point Objectives
  - Automate your backups
- Keep copies offsite or in the cloud
- Test your recovery processes to ensure that they work!

## POLL QUESTION #3

Do you have an incident response plan (IRP) in the event of a cyber attack?

a) Yes

b) No

c) Don’t know

d) What is an incident response plan?

# Tips for enhancing cyber security: Incident Response Plan

- A well-defined incident response plan allows you to
  - Effectively identify an incident
  - Minimize the damage
  - Reduce the cost of a cyber attack
    - Ponemon Institute’s “Cost of a Data Breach” Report indicated that having an IRP saved orgs an average of 35%.
  - Find and fix the cause to prevent future attacks
  - Meet your compliance and regulatory requirements

National Institute of Standards and Technology (NIST) provides detailed steps to implement an Incident Response Plan NIST-800-61

https://www.nist.gov/cyberframework

# Tips for enhancing cyber security: Managed Security Services (Outsourcing)

- Leveraging a Security provider for all of your security needs may be a viable option
  - Deploy out of the box security solutions
  - Allows you to meet your security needs quickly
  - May reduce upfront capital investment
  - Enables you to focus on your core business functions
- Key considerations for selecting security provider
  - Can they meet your end to end security needs?
  - Identification of where data is to be stored and restrictions
  - Support model and offshore considerations
  - Reporting and Alerting for threats
  - Service Level Agreements for patching/ vulnerability remediation
  - Do they meet your Compliance and Audit needs?
  - Indemnification and limitations on liability as they relate to data privacy, cybersecurity, and breaches
  - Termination provisions regarding destruction and/or return of data

## POLL QUESTION #4

Currently, my business:

a) Has no cyber insurance – not really considering purchase
b) Has no cyber insurance – strongly considering purchase
c) Has a cyber endorsement or policy – don’t plan on renewing
d) Has a cyber endorsement or policy – plan on renewing
e) Has a cyber endorsement or policy – considering buying more coverage or limit
f) Don’t know

# Tips for enhancing cyber security: Cyber Risk Insurance

- Agents are a source of information on cyber exposure
- Policy is in addition to prevention and mitigation (not instead of)
- What it covers – main components, including third party
  - Data Breach
  - Ransomware
  - Business Interruption
  - Business Email Compromise (not standard/low limits)
  - Third Party Liability
- How it can reduce overall cost of attack/benefits of insurance
- Access to risk management solutions through insurance carrier

# Key takeaways

- No organization is immune from a cyber attack
- Understanding exposure is critical to know how to protect
- Employee training and awareness is half the battle
- Every additional measure taken to protect adds up
- Not every cybersecurity process is complicated or expensive
- Have an incident response plan in place to help mitigate a loss
- Talk to your agent about cyber risk exposure and consider insurance
- Cyber exposure is very dynamic, so staying informed is important
  - Business Solutions Center at Nationwide
  - https://bsc.nationwide.com/

# Thank you for joining us!

# Sources

- https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf
- https://www.juniperresearch.com/press/press-releases/cybersecurity-breaches-to-result-in-over-146-bn https://www.databreachninja.com/wp-content/uploads/sites/63/2019/03/2018-NetDiligence-Claims-Study.pdf
- https://www.fireeye.com/solutions/small-and-midsize-business.html
- https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf
- https://www.insurancebee.com/blog/smb-owners-unprepared-for-cybercrime
- https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/
- https://www.coveware.com/blog/q1-2020-ransomware-marketplace-report
- https://pdf.ic3.gov/2019_IC3Report.pdf
- https://securityintelligence.com/posts/whats-new-in-the-2019-cost-of-a-data-breach-report/
- https://cve.mitre.org/
- https://www.nist.gov/cyberframework