Moderated by Daniel Eliot, Director
Small Business Programs
National Cyber Security Alliance

Sara Robben, Statistical Advisor
National Association of Insurance Commissioners

Angela Gleason, Senior Counsel
American Insurance Association
Be a Part of Something Big

Get involved and promote a safer, more secure internet.

www.staysafeonline.org
Goal of 5-Step Approach Is Resilience

Know the threats and **Identify** and **Protect** your assets

**Detect** problems and **respond** quickly and appropriately

Know what **recovery** looks like and prepare

Thanks to our National Sponsors

MediaPRO
Cybersecurity & Privacy Education

TREND MICRO™
Initiative for Education
DIGITAL SAFETY OUTREACH
Sara Robben, Statistical Advisor
National Association of Insurance Commissioners
<table>
<thead>
<tr>
<th>Number of Internet Users</th>
<th>• 4.2 Billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Google Searches per day</td>
<td>• 3.5 Billion</td>
</tr>
<tr>
<td>Number of Active Twitter Users</td>
<td>• Over 340 Million</td>
</tr>
<tr>
<td>IoT’s</td>
<td>• Approximately 17 Billion for 2018</td>
</tr>
<tr>
<td>Internet</td>
<td>• Over 50% of all Internet traffic is from an automated source</td>
</tr>
</tbody>
</table>
Are Small Businesses at Risk for a Cyber Attack?

- Small businesses reporting attacks in 2017
  - 47% reported one attack
  - 44% reported two to four attacks
- 2/3 of these businesses did not strengthen their security following an attack
- 7 out of 10 businesses aren’t prepared to handle cyber attacks

Survey Source: Hiscox
Types of Attacks

• Malware
• Ransomware
• Phishing
Social Engineering Red Flags

**FROM**
- I don't recognize the sender's email address as someone I ordinarily communicate with.
- This email is from someone outside my organization and it's not related to my job responsibilities.
- This email was sent from someone inside the organization or from a customer, vendor, or partner and is very unusual or out of character.
- Is the sender's email address from a suspicious domain (like micorsoft-support.com)?
- I don't know the sender personally and they were not vouched for by someone I trust.
- I don't have a business relationship nor any past communications with the sender.
- This is an unexpected or unusual email with an embedded hyperlink or an attachment from someone I haven't communicated with recently.

**TO**
- I was cc'd on an email sent to one or more people, but I don't personally know the other people it was sent to.
- I received an email that was also sent to an unusual mix of people. For instance, it might be sent to a random group of people at my organization whose last names start with the same letter, or a whole list of unrelated addresses.

**DATE**
- Did I receive an email that I normally would get during regular business hours, but it was sent at an unusual time like 3 a.m.?

**SUBJECT**
- Did I get an email with a subject line that is irrelevant or does not match the message content?
- Is the email message a reply to something I never sent or requested?

**ATTACHMENTS**
- The sender included an email attachment that I was not expecting or that makes no sense in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly dangerous file type. The only file type that is always safe to click on is a .txt file.

**CONTENT**
- Is the sender asking me to click on a link or open an attachment to avoid a negative consequence or to gain something of value?
- Is the email out of the ordinary, or does it have bad grammar or spelling errors?
- Is the sender asking me to click a link or open up an attachment that seems odd or illogical?
- Do I have an uncomfortable gut feeling about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a compromising or embarrassing picture of myself or someone I know?

© 2017 KnowBe4, LLC. All rights reserved. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies.
Potential Impacts to a Business as the result of a cyber incident

- Financial Loss (47%)
- Information Breach/Theft (35%)
- Reputation/Brand Image Issues (14%)
- Regulatory/Governance and Legal Issues (4%)

Source: Insurance Information Institute
Protection Measures

- Backup your data
- Update Operating Systems and other software
- Passwords
- NIST
- Hire an IT consultant
- Educate your staff
Data Breaches and How Insurance Helps

• Cyber-Related losses over the past year cost $188,400 on average (Source: J.D. Power)
• Business interruption is the most common type of loss from a cyber incident
• Businesses also experience data loss or corruption, as well as data breach losses
• Regulatory/Governance and Legal Issues (4%)
• Most small businesses affected by a breach said their cyber insurance was adequate

Source: Insurance Information Institute
Cyber Insurance

- Businesses with cyber insurance often have similar coverages
- Cyber coverage can be combined with other coverages
- Cyber insurance uptake is still a work in progress
- Many businesses do not think they need cyber insurance; however, they don’t believe they can handle threats
- Cyber insurance is still poorly understood
- Many insurers offer cyber insurance or service

Source: Insurance Information Institute
Small Business Information Security: The Fundamentals


Multi-factor Authentication Basics


Backup Basics

- https://www.pcmag.com/article2/0,2817,2363057,00.asp

Phishing


Password Managers

- https://www.lastpass.com
- https://www.logmeonce.com/
CyberSecure™
MY BUSINESS
PLAN. PROTECT. RESPOND.

NATIONAL CYBER SECURITY ALLIANCE
Small Business Cybersecurity Insurance

Angela Gleason, Senior Counsel
American Insurance Association
Cyber as a Peril

Cybersecurity incidents are a peril - the risk or cause of loss for which insurance coverage is sought.
“Cyber Insurance”

The product typically referred to as “cyber insurance” is more often referred to in the insurance world as a network security and privacy type of policy that typically provides first and third party coverage for costs arising from defined unauthorized cyber events.
First Party Coverage Examples

Insurance that applies to the business’s own losses.

- Notification Costs
- Investigation and Public Relation Expenses
- Costs associated with business interruption, theft, and equipment or data restoration
Third Party Coverage Examples

Insurance that applies to the costs and damages associated with third party claims.

• Lawsuit Liability
• Regulatory Investigations
• Fines and Penalties
Where do I begin?

- Understand the risks and consequences your business faces from cyber events
- Understand your current insurance portfolio/coverages
- Have a conversation with your insurer and broker
Components of a Cyber Insurance Policy

• Coverage Grants
• Exclusions
• Coverage Limits
• Pre and Post Services
Benefits of Cyber Insurance

- Risk Transfer Mechanism
- Risk Analysis Tool
- Pre and Post Breach Resources
Takeaways

Don’t consider cyber insurance a check the box exercise.

Make security part of your culture.

Ask your insurer and broker questions.
Webinar Series
Second Tuesdays
2:00 p.m. EDT

Up-Coming Webinars:
• December 11th “New Small Business Cyber Resources for the New Year”
• more webinar topics coming soon

To Register: www.staysafeonline.org
NATIONAL CYBER SECURITY ALLIANCE
Small Business Cybersecurity Insurance

National Association of Insurance Commissioners
https://www.insureuonline.org/

Signature Sponsor
Trend Micro
www.trendmicro.com

The American Insurance Association
http://www.aiadc.org/

Contributing Sponsor
MediaPRO
https://www.mediapro.com/SMB

National Cyber Security Alliance
www.staysafeonline.org/cybersecure-business