ENTERPRISE RISK MANAGEMENT
A Strategic Approach

Board of Directors Meeting – American Bus Association
September 24, 2019

Thomas DeMatteo
Chief Legal Officer, General Counsel & Secretary
ABC Bus Companies, Inc.

Michelle Wiltgen, AVP – National Marketing Manager
National Interstate Insurance
Richfield, Ohio

Julie Proscia, Partner
Smith Amundson Law Firm
Chicago, Illinois

Bennet Hammer, President
Hammer IT Consulting
What is Enterprise Risk Management? ("ERM")

A strategic analysis of risk throughout an organization that cuts across business units and departments and considers end to end processes.
TRADITIONAL (Silo) vs. ERM (Holistic)

Examples of Silo Structure:
- Audit committee on financial risks
- Legal department on regulatory compliance
- IT department on technology risk
- Insurance department on coverage risks

Silo Structure May Miss:
- Cross functional risks
- Industry wide risks
- Political risks
- Reputational or brand risks
TRENDS PUSHING “ERM”

- Greater Transparency Generally
- Insurance Carrier Requirements
- Financial Disclosure
- Rating Agencies
- Globalization
- Security and Technology
- Disaster Preparedness
- Increased Regulatory Scrutiny
TRENDS PUSHING “ERM” (con’t.)

For Example:

• Wall Street rules require disclosure about a company’s risk management practices, to include:
  • The board’s role in the oversight of risk and the effect, if any, that this has had on the company’s leadership structure.
  • The relationship between a company’s compensation practices and risk management.
WHAT KEEPS YOU UP AT NIGHT?

Types of Risk

• Operational
• Strategic
• Financial
• Compliance
• Legal

• IT/Cyber Security
• Reputational
• Environmental
• Political
Basic Elements of ERM Plan

To set up an ERM program, a company needs to:

• Identify the risks faced at all levels of the company
• Likelihood of occurrence
• Quantify potential impact
• Interrelationship to each other
• Define risk appetite or tolerance
• Develop a framework for managing the risks, with a view to conforming behavior and decision making within the stated risk appetite
Determining Risk Tolerance/Appetite

The following factors should be considered when setting risk appetite:

- Shareholder expectations
- Willingness to accept earnings volatility
- Financial capacity to withstand loss
- Willingness to expand product/service range and geographical coverage
- Potential for growth through acquisitions
- Desired credit rating
- Risks considered absolutely unacceptable
Benefits of ERM

Enterprise risk management offers a number of benefits:

• Aligns risk appetite and corporate strategy
• Links growth, risk, and returns
• Improves risk responses
• Reduces operational surprises and losses
• Manages enterprise-wide risks
• Recognizes and acts upon opportunities
• Deploys resources effectively
STRATEGIC NEEDS

OWNERSHIP BUY-IN WITH RESOURCES

+ 

CRISIS MANAGEMENT PROGRAM

+ 

SOPHISTICATED INSURANCE COVERAGE
Crisis Communications

1. The time for decision making is drastically compressed

- The dangers of “siloed” organizations are greatly expanded
- Demands greater preparation in advance
2. The “media” can be anyone, anywhere

- Social Media – Facebook, Twitter, etc.
- The BAD NEWS- a vendor, employee, customer- ANYONE- can write or produce a story
- The GOOD NEWS- organizations also have more power to tell their own stories
3. Audiences are increasingly sophisticated and skeptical

- Everyone has seen this play too many times
- Incomplete answers, no answers, reluctant answers and false answers are deadly
4. There are no barriers or borders in a crisis

- The worlds of media, legislation, litigation, regulation, consumer, and financial all overlap

- Geography is increasingly less important- a problem in one market is a problem in every market
5. Damaged reputations can be restored more quickly than before

- With the right focus and resources
- And with real transparency and candor
How Many Devices are Connected to the “Internet of Things”?
• The Internet of Things refers to the rapidly growing network of connected objects that are able to collect and exchange data using embedded sensors.

• Gartner Analytics estimates 26 billion devices in 2020, growing to 100 billion
Types of Cyber Attacks

• Phishing (Email Scams)
• Denial of Service
• Man in Middle
• Insider Attack
• Password Attack

• Injection Attack
• Cross Sites Attack
• Eavesdropping
• Malware
Key Questions

Go home and ask yourself do you have Personal Identifiable Information (PII) on your system?

Definition of PII as follows: An individual’s first name or first initial and last name in combination with any one or more of the following data elements:

- Social security number
- Driver’s license or state issued identification card number
- Account number, credit card number or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account
- Medical information (any information regarding an individual’s medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional)
- Health insurance information (an individual’s health insurance policy number or subscriber identification number, and unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records); or
- Information or data collected through the use or operation of an automated license plate recognition system (a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data).
Cyber Security Key Takeaways

High Risk to Companies and Customers
• Corporate reputation/liability; aggressive enforcement climate
• Customer privacy – core public policy focus in US and EU

Broad Oversight Critical
• Management focus and resource allocation
• Robust Enterprise Risk Management (ERM) program, internal controls and testing
• Consider Cyber Insurance Policy
• Regular (at least semi-annual) updates to Board

When an Event Occurs
• Management must undertake immediate and reasonable effort to understand facts
• Disclose to Board and affected stakeholders ASAP
• Compliance with laws and regulations and every state likely has nuances
Types of Commercial Insurance (Spreading of Risk)

- Property
- General Liability
- Auto
- Income
- Workers' Compensation
- Employment Practices
- Crime
- Cyber Security Insurance
- Professional Liability
- Ocean/Inland Marine
- Equipment Breakdown
- Directors and Officers
- Difference in Conditions
- Umbrella
- M&A Insurance
Insurance and Risk Financing Options

- Traditional Insurance
- Deductible Programs
- Self Insurance
- Captives
- Risk Retention Groups
Benefits of Insurance

• Protects net worth of Business and Owners
• Reduces financial uncertainty
• Provides access to claims administration and safety services
• Satisfies legal and regulatory requirements
• Easy to access
• Flexible
Enterprise Risk Management
Protecting Your Company
Meet The Presenter

• Michelle Wiltgen
• AVP & National Marketing Manager
  ◦ National Interstate Insurance Company – the leading provider of insurance to the Passenger Transportation Industry
  ◦ In the business for 35 years – 28 of them in passenger transportation
  ◦ Holds a BA in Management & Labor Relations from CSU
Topics for today

✓ Current insurance marketplace
  ◦ How did we get here?
✓ How can you protect your company?
✓ What can you do?
Outlook - Continued elevated loss and combined ratios, driven by adverse loss frequency and severity trends and unfavorable prior-year reserve development.
Rates - Commercial auto insurers continue to raise rates in response to the adverse loss frequency and loss severity trends
Underwriting results - The commercial auto combined ratio was an estimated 110.4% in 2018. This was the eighth consecutive year with a combined ratio above 100%.
Only THREE of the top 50 commercial auto liability insurers have a combined ratio under 100:*  

✓ Progressive Insurance (1): 85.7  
✓ Chubb (8): 92.0  
✓ Great American (19): 90.7  

* Information obtained from Conning Insurance Segment Report - Mid-Year 2019
Loss frequency is rising due to:

- Higher vehicle utilization
- Distracted driving
- Deteriorating road conditions
- Poorer driver profile - companies are hiring less experienced/less qualified drivers causing more accidents
Loss severity - and “frequency of severity” continue to be among the most pressing concerns for commercial auto insurers.

Numerous seven and eight figure court awards have fed plaintiff attorney interest in pursuing accident litigation.

Increased attorney advertising and growth in litigation funding have also contributed to the rising loss severity trend.

Adverse development: In 2018, the industry experienced $1.8 billion of adverse development for commercial auto/truck medical.

* Information obtained from Conning Insurance Segment Report - Mid-Year 2019
The outlook for commercial auto is for continued poor underwriting results from adverse loss trends.

Adverse trends are driving insurers to take underwriting actions including:
- Re-underwriting
- Nonrenewal of underperforming policies or segments

Industry reports indicate that challenging commercial auto classes include trucking for hire, tow trucks, nonemergency medical transportation, and charter buses.
Protecting your company

Choose “best in class” partners:

✓ Broker/Agent
✓ “A” Rated by A.M. Best Insurance Companies
✓ Insurance coverage/limits to protect your business
Choose your broker/agent wisely

- **What is their motivation?**
  - Are they a broker or an agent?
  - How are they paid, how much, and by whom?
  - What markets do they represent?
  - What is their relationship with those markets?
  - Do they find you a new insurance company every year?
  - Do **YOU** know who the insurance company is?
  - Do they challenge your decisions? Are you willing to let them?
Choose your insurer(s) wisely

- All insurance companies are **not** equal:
  - Underwriting & Claims expertise and philosophy
  - Commitment to the industry
  - Coverage and service options that fit your business model and appetite for risk
  - You may need to work with more than one producer to get access to all desired insurance markets
  - Financial rating
  - Stability
  - Reputation
AM Best was founded in 1899 by Alfred M. Best with the mission to report on the financial stability of insurers and the insurance industry. It is the oldest and most widely recognized provider of ratings, financial data and news with an exclusive insurance industry focus.

Best's Credit Ratings, which are issued through A.M. Best Rating Services, Inc., are a recognized indicator of insurer financial strength and creditworthiness.
How many insurance companies are there in the United States?

Rating Categories:
- Superior   A+ or A++
- Excellent   A or A-
- Good        B+ or B++
- Fair        B or B-
- Marginal    C+ or C++
- Weak        C or C-
- Poor        D
• How many insurance companies are rated:
  
  A+ or better: 27%
  A or better: 65%
  A- or better: 92%

• Do you know what rating(s) your insurers have?
• How much insurance is REQUIRED vs. what you NEED to protect your company?
• How much insurance is enough?
• Flood insurance – do you have it? do you need it?
• Is your total fleet value over $1mil?
  ◦ Excess physical damage
• Do you use computers?
  ◦ Cyber liability
Do your homework

• Know what’s covered
• Punitive Damage Claims
  ◦ “Nuclear verdicts”
  ◦ Punish the wrongdoer
  ◦ Some states do not allow insurance policies to cover; some policies may exclude
• Could you be negligent in managing safety?
Risk Financing Options

• Traditional Insurance
  ◦ First Dollar
  ◦ Deductible

• Alternative Risk Financing
  ◦ Captives – Group or Single Cell

• Self Insurance
What can you do?

• Treat your broker/agent like the consultant/business partner that they are
  ◦ Meet regularly
    ➢ Not just at renewal time
  ◦ Request/require regular claims reviews
    ➢ With your broker and insurer
Be prepared, start early

• Quality insurers want the same information every year – manage it
• Your renewal discussion should be 90 days prior to your effective date, not 9 days
• Your renewal application should be submitted 60 days prior to your effective date, not 6 days
• You own your loss runs – don’t tolerate delays or gamesmanship
Own your information

• Review your info to confirm accuracy
• Correct items that need updating
  ◦ Are the unit counts correct?
  ◦ Are your vehicle values current?
  ◦ Do your IFTA’s match your application?
• Provide a summary of your business history and future plans
• Does your website match your submission info?
• Do you have a copy of what is submitted on your behalf?
The absence of accidents is not the presence of safety

- Proactive Safety Tools & Resources
  - Sufficient safety staffing
  - Discipline and coaching protocols
  - AERs
  - PATs
  - Return to Work Programs
- Industry Involvement
  - Associations
  - Reputation
- CSA Scores – fluctuation, alerts, safety rating, etc
Tell us your story

• Insurance Submissions – Paint the picture
  ◦ Complete info
  ◦ Accurate info
  ◦ Include business growth/future plans

• Lower confidence in the information can drive up premiums or be the grounds for declination
One size does not fit all

✓ Know the insurers
✓ Know the options available
  ◦ Coverages
  ◦ Risk management services
  ◦ Claims service/philosophy
Questions?

Michelle Wiltgen
O: 800-929-1500 x1213
M: 440-821-1961
Michelle.Wiltgen@natl.com
www.natl.com
EEOC Trends
Social Media in the Workplace
Social Media in the Workplace

- Private Sector employers **can:**
  - Create a social media policy that sets expectations for how employees should use social media.
  - Monitor work computer use for internet use.
- Private Sector employers **cannot:**
  - In most states, employers cannot ask for your password and username to social media accounts. 20 states have enacted legislation prohibiting this. So far, there is no federal law that prohibits it.
  - In some states, like Michigan and Illinois, employers cannot gather or keep information of an employee’s communications or non-employment activities, without the employee consent (with few exceptions).
  - Fire an employee for social networking and social media usage if it is “concerted activity” for the purpose of collective bargaining, mutual aid or protection.
To Friend or Not to Friend

- Generally, managers should NOT friend other employees on social media.
  - Sending a friend request puts an employee in an uncomfortable position.
  - You will have access to sensitive information.
    - Can see employees posts about political views, religion, lifestyle preferences, medical or health issues.
    - Opens the door to discrimination or harassment.
  - Can add to your professional responsibilities.
  - Most social media posts are too personal for work.
Social Media in the Workplace

- Employers can screen candidates’ **public** social media accounts, BUT comes with consequences:
  - Cannot have an employee “friend” or “follow” a candidate to view their **private** account.
  - 70% of employers screen candidates’ social media accounts during the hiring process.
  - Potential danger in unknowingly collecting protected information like age, skin color, race, gender, religion, etc.
    - This can create a bias or discrimination problem.
Social Media in the Workplace

- Can Employers fire an employee for social media posts?
  - Most employees are “at-will” employees, employer can terminate for any reason that is not illegal or in violation of a contract.
  - But, not always a good idea to terminate based on social media posts. Each situation needs to be considered on a case-by-case basis.
    - Posts about company information or negative comments about your job/clients will tend to be grounds for termination.
    - Potential to violate state and federal laws for firing an employee due to off-duty social media posts.
Trends of Ageism

- Age based EEOC complaints are rising steadily due to the continued increase of older workers in the job force.
  - More baby boomers are staying in the workforce longer due to the Recession that left many unemployed or depleted their retirement savings.
- In 2017, 18,376 age discrimination complaints were filed with the EEOC.
- Age based harassment claims have tripled in 2017 compared to 1992.
  - Job postings may tend to prefer young workers who are “digital natives” and familiar with technology
- Significant jump in age based discrimination charges in 2010 data due to the Recession.
Trends of Ageism

ADEA Charges Alleging Age and Race, Age and Sex, Age and Disability Discrimination
#MeToo National Trends
#MeToo Timeline

1997
- Tarana Burke
- Access Hollywood Tape

2006
- Judge rules in favor of Taylor Swift

2016
- Just Be Me Inc.
- Harvey Weinstein (42 women)

Aug. 2017
- “If you have been sexually harassed or assaulted, write #MeToo and reply to this Tweet” - Alyssa Milano

Oct. 5 2017
- McKayla Maroney – Larry Nassar (265)

Oct. 15 2017
- McDonald’s workers walkout in protest

Oct. 18 2017
- Bill Cosby Convicted

April 2018
- Kavanaugh Hearings – Dr. Blasey Ford

Sept. 2018
- Google workers walk out in protest

Sept. 2018
- Midterm Elections

Nov. 2018
- 2019
#MeToo National Trends

- Recent statistics from the EEOC
  - Sexual harassment charges with the EEOC increased by over 12% from the previous calendar year; the first increase in harassment complaints in a decade.
  - Sexual harassment lawsuits filed by the EEOC increased by 50% since 2017.
  - The total recovery for sexual harassment complainants rose from $47.5 million in 2017 to approximately $70 million in 2018.
  - In the last year, website traffic to the EEOC’s sexual harassment page more than doubled.
EEOC Charges Of Sexual Harassment Climb

For the first time this decade, the U.S. Equal Employment Opportunity Commission had an increase in sexual harassment complaints.

Source: U.S. Equal Employment Opportunity Commission
#MeToo National Trends

- Movement to individual liability, i.e. California and Illinois.
- Movement to direct access to court.
- Movement to mandated training.
- Changes in the perception of what is and is not reasonable workplace behavior.
What States Have Done

- **IL**: Requires harassment trainings for all employees, limits the use of policies or agreements intended to prevent employees from reporting sexual harassment, made harassment against contract workers illegal, prohibits union representatives from representing both a victim of sexual harassment and the harasser.

- **NY**: The new law lowers the burden of proof for harassment claims. Any harassment based on a protected class, or for participating in protected activity, will be unlawful “regardless of whether such harassment would be considered severe or pervasive under precedent applied to harassment claims.”
What States Have Done

- **TN:** Prohibits employers from requiring employees and job applicants to sign non-disclosure agreements about sexual harassment as a condition of employment.

- **OR:** Significantly increased the statute of limitations within which an aggrieved employee may file a lawsuit or administrative claim alleging, among other things, discrimination on the basis of race, color, religion, sex, sexual orientation, national origin, marital status, age, uniformed service, or disability.

- **VT:** A new law prohibits businesses from requiring employees to sign away their right to report or sue for sexual harassment, and prohibits settlement agreements from including provisions that say the employee cannot work for the business in the future.
States with Mandatory Harassment Training

- **California:**
  - Currently, companies with 50 or more employees must provide 2 hours of training every 2 years for supervisory employees. New supervisory employees, upon assumption of position, must be trained within 6 months. Employers can keep supervisors on their individual two-year training date or designate a “training year” where all supervisors are re-trained.
  - By January 2021, companies with 5 or more employees must train all workers. There are two types of training, one for supervisors and one for employee non-supervisors. Training must be done every two years.
  - Any employee hired to work less than 6 months shall be trained within 30 days after their hire date, or within 100 hours worked. Temporary workers employed by a temporary agency must be trained by the agency -- not the client.
States with Mandatory Harassment Training

- **Connecticut:**
  - Must be completed within 6 months of starting as a manager for companies with 50 or more employees.

- **Delaware:**
  - Must be completed by Jan. 2020 for existing employees & within one year of start for new employees. Companies with 50 or more employees must train every two years.
States with Mandatory Harassment Training

- **Illinois:**
  - Effective Jan. 1, 2020 all employees must be trained annually.

- **Maine:**
  - Must be completed within one year of hire and one year of starting a management role. For companies with 15 or more employees.

- **New York:**
  - Must be completed by Oct. 2019 for NY State and April 2020 for NY City. All employers in the state of NY must provide annual training. In NY City, companies with 15 or more employees must provide annual training.
States with Mandatory Harassment Training

- **For State Employees Only:** Kansas, Kentucky, Louisiana, Mississippi, Nevada, New Jersey, North Carolina, Pennsylvania, Tennessee, Texas, Utah, Washington.
Tips for what Employers Should Do

• Have an investigation plan.
  • Must be thorough and timely.
  • Policies must be followed no matter what.
• Train more, but outside of the box.
  • Train on sexual harassment policies and procedures.
  • Train on reporting system(s).
  • Create an environment that is open and inclusive.
  • Train on hiring practices – diversity and inclusion.
  • Train on and develop inclusion programs.
Marijuana in the Workplace
National Trends on Marijuana Recreational/Adult Use

- **Lawful in 11 States + DC** – Alaska; California; Colorado; Illinois; Maine; Massachusetts; Michigan; Nevada; Oregon; Washington; District of Columbia; Vermont.

- **Decriminalized in 14 States (i.e. possession of small amounts result in civil offense, not a criminal offense)** – Connecticut; Minnesota; Missouri; North Carolina; Maryland; Delaware; Illinois; Ohio; Rhode Island; Nebraska; Mississippi; New York; New Hampshire; New Mexico.

- **Misdemeanor in 12 states** – Kansas; South Dakota; Utah; Virginia; West Virginia; Wyoming; Idaho; Tennessee; Kentucky; Wisconsin; Indiana; South Carolina.

**Excludes local ordinances decriminalizing/reducing penalties for marijuana use/possession.**
Marijuana & the Workplace

• Employers may enforce drug testing policies, zero tolerance policies, and drug free workplace policies, even in states where medical and recreational use is permitted.
  • The policies must be applied in a nondiscriminatory manner.

• The policies can prohibit employees from using, possessing, or being impaired while at work or while on call.

• The workplace can also be defined beyond the employer’s physical building.
Marijuana Use & Drivers

• If an employee is a Department of Transportation (DOT) employee, they must comply with FMCSA regulations for drug testing.
  • DOT does not authorize “medical marijuana” under a state law to be a valid medical explanation for a transportation employee’s positive drug test result.
  • DOT does not authorize the use of Schedule I drugs, including marijuana, for any reason, even in states where “recreational use” is permitted.
  • Prohibits use even if off duty.
Thank You!!

Julie A. Proscia
SmithAmundsen LLC – Partner
jproscia@salawus.com
(630) 587-7911

MANAGEMENT-SIDE
LABOR & EMPLOYMENT COUNSEL

www.laborandemploymentlawupdate.com

Chicago, St. Charles, Rockford, Woodstock, Indianapolis, Milwaukee, St. Louis. USLawNetwork Member.

11/30/2016
Cybersecurity Presentation

by

Bennet Hammer, President

Hammer IT Consulting
Cybersecurity: A Problem Too Big for Companies to Ignore

Presented by Dr. Bennet Hammer
President of Hammer IT Consulting, Inc.
About the Speaker

▪ Founder and President of Hammer IT Consulting, Inc.

▪ Earned a doctorate degree in Information Systems with a concentration in Information Security

▪ IT and Security Consulting Company

▪ Provide IT hardware, security software and security service solutions to State and Local Government, Higher Education, K-12, Healthcare, and Corporate Entities throughout the United States.
Companies Who Have Been Breached

JUST A RECAP OF COMPANIES WHO HAVE BREACHED
Cyber-crimes are increasing for businesses of all sizes

- 70% of data breaches happen to small and medium businesses

- 39% of the global data breaches caused by malware were ransomware

- 58% of SMBs have experienced a data breach in the last 12 months

- Malicious hackers are now attacking computers and networks at a rate of one attack every 39 seconds

- It takes 6 months on average to detect a data breach for companies that don’t have a security program
Why Are Cyber Attacks On The Rise?

- Increased Attack Surfaces
  - Smart Phones
  - Tablets
  - IoT Devices

- Lack of Training

- Evolving Technologies

- Lack of 3rd Party Due Diligence

- Cybercrime is a growth business

- Shortage of Cyber Professionals

- Insider Threats

- Paralysis – Not doing anything

- Lack of Management Support
# Types of Threats

<table>
<thead>
<tr>
<th>Malware</th>
<th>Software that is designed to gain unauthorized access or to cause damage to a computer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware</td>
<td>Type of malicious software. It is designed to extort money by blocking access to files or the computer system until the ransom is paid. Paying the ransom does not guarantee that the files will be recovered, or the system restored.</td>
</tr>
<tr>
<td>Phishing</td>
<td>The practice of sending fraudulent emails that resemble emails from reputable sources. The aim is to get you to do something (open an attachment, click a link, give sensitive data like credit card numbers and login information). It’s the most common type of cyber attack.</td>
</tr>
<tr>
<td>Crypto jacking</td>
<td>The unauthorized use of someone else’s computer to mine cryptocurrency. Hackers do this by either getting the victim to click on a malicious link in an email that loads crypto mining code on the computer, or by infecting a website or online ad with JavaScript code that auto-executes once loaded in the victim’s browser.</td>
</tr>
<tr>
<td>Zero Day</td>
<td>Takes advantage of a security vulnerability before the vulnerability becomes generally known. There are zero days between the time the vulnerability is discovered and the first attack.</td>
</tr>
<tr>
<td>Social Engineering</td>
<td>Social engineering is a tactic that adversaries use to trick you into revealing sensitive information. They can solicit a monetary payment or gain access to your confidential data. Social engineering can be combined with any of the threats listed above to make you more likely to click on links, download malware, or trust a malicious source.</td>
</tr>
</tbody>
</table>
Who are the attackers?
Internal Attackers

**Internal Attackers – The Usual Suspects**

- Disgruntled Employees
- Unintentional
- Thieves/Corporate Espionage

<table>
<thead>
<tr>
<th>WHO STEALS THE MOST?</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sales</td>
<td>24%</td>
</tr>
<tr>
<td>IT</td>
<td>20%</td>
</tr>
<tr>
<td>Finance &amp; Accounting</td>
<td>10%</td>
</tr>
<tr>
<td>Marketing &amp; Communications</td>
<td>8%</td>
</tr>
<tr>
<td>Other</td>
<td>38%</td>
</tr>
</tbody>
</table>
External Attackers

- Organized Attackers
  - Terrorists
  - Hacktivists
  - Nation State
  - Criminal Actors

- Hackers
  - Black Hat
  - White Hat
  - Gray Hat

- Amateurs
How they attack?
Tools

Malicious Software (Malware)
- Virus
- Worm
- Trojan Horse / Logic Bomb
- Rootkits
- Botnets / Zombies

Social Engineering
- Phishing
- Baiting
- Phone Hacking / Vishing
- Shoulder Surfing
- Dumpster Diving
- Tailgating
Social Engineering

Social Engineering is the psychological manipulation of people to obtain confidential information. Information may be obtained by:

- Baiting the target
- Creating distractions
- Creating a sense of urgency
- Using props and locations to their advantage
- Asking for help
- Creating realistic scenarios
E-Mail Security
Was Your E-mail Hacked?

EMAIL HACKED? – THE WARNING SIGNS

Your contacts tell you they’re receiving spam emails from you

You receive multiple failed delivery emails

Hey!!

Buy ????? NOW!

There are messages in your sent folder that you did not send

Your accounts location login history doesn’t match your recent activity
E-mail Phishing Example

All:

Due to unexpected system outages, we will need to limit access to our email servers on **Thursday, September 19, 2019 from 10am until 6pm**.

Contingent and part-time employees will not have access to email during that time.

All email users will need to request access to their email by **COB** tomorrow. Please be sure to adding your name to the following list: [http://www.customername.com/requestaccess](http://www.customername.com/requestaccess). Please be sure to request access by COB today. Employees that do not request access will be unable to send and receive email during the outage on Tuesday.
Passwords
Password Length

Adding a single character to a password boosts its security exponentially. In a so-called “dictionary attack,” a password cracker will utilize a word list of common passwords to discern the right one.

<table>
<thead>
<tr>
<th>Characters</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>.29 Milliseconds</td>
</tr>
<tr>
<td>8</td>
<td>5 Hours</td>
</tr>
<tr>
<td>9</td>
<td>5 Days</td>
</tr>
<tr>
<td>10</td>
<td>4 Months</td>
</tr>
<tr>
<td>11</td>
<td>1 Decade</td>
</tr>
<tr>
<td>12</td>
<td>2 Centuries</td>
</tr>
</tbody>
</table>
How To Create Complex Passwords

- Don’t use dictionary words
- Use upper and lower case characters
- Don’t use your username
- Don’t use personal information such as your name, address, or significant dates. e.g. birthdays, anniversaries, etc.

Use at least one numeric character
Incorporate special characters such as $, &, and %

ILb0&pp-xtr@ch

Use at least 12-14 characters

Creating an anagram of a sentence you can remember is usually the easiest way to remember your complex password

“I love black olive and pepperoni pizza with extra cheese”
Create Unique Passwords For Each Account

It’s easier than you think!

A 2 letter delimiter at the end of a complex password can make it unique for every account/website and will strengthen the complexity by adding additional characters.

<table>
<thead>
<tr>
<th>Complex Password</th>
<th>Outlook Account</th>
</tr>
</thead>
<tbody>
<tr>
<td>ILb0&amp;xtr@ch</td>
<td>ILb0&amp;xtr@chou</td>
</tr>
<tr>
<td>Yahoo</td>
<td>ILb0&amp;xtr@chya</td>
</tr>
<tr>
<td>Google</td>
<td>ILb0&amp;xtr@chgo</td>
</tr>
<tr>
<td>Salesforce</td>
<td>ILb0&amp;xtr@chsf</td>
</tr>
<tr>
<td>Facebook</td>
<td>ILb0&amp;xtr@chfb</td>
</tr>
</tbody>
</table>
Passwords In General

For passwords to be an effective measure against cyber attackers, the following should be adhered to:

- Passwords need to be complex
  - Should use a combination of uppercase and lowercase letters, numbers, special characters, e.g. @, #, -, _, $, !
  - Should be at least, 12-14 characters in length
- Passwords should be unique and different for every account that requires a password
- Passwords should never be shared; with anyone!
- Passwords should never be written down
Hammer’s Recommendations

1. Be careful what you click on!
2. Backup your data regularly and check the backup.
3. Patch promptly.
4. Protect all endpoints including mobile devices.
5. Encrypt sensitive data.
6. Use two-factor authentication.
7. Don’t forget physical security (Surveillance Cameras).
8. Create Unique Passwords.
10. Plan, Plan, Plan ...
Thank You

Comments and Questions?
Contact

Dr. Bennet Hammer
(941) 716-0045
bennet@hammeritconsulting.com
http://hammeritconsulting.com
Presenters Contact Information

Julie Proscia, Attorney, Smith Amundson
jproscia@salawus.com
630-587-7911

Michelle Wiltgen, AVP – National Marketing Manager
National Interstate, michelle.wiltgen@natl.com
1-800-929-1500, ext. 1213

Thomas DeMatteo
Chief Legal Officer, General Counsel & Secretary
ABC Bus Companies, Inc.
tdematteo@abc-companies.com
1-800-222-2875

Bennet Hammer, President
Hammer IT Consulting
Bennet@HammerITConsulting.com
833-426-6374