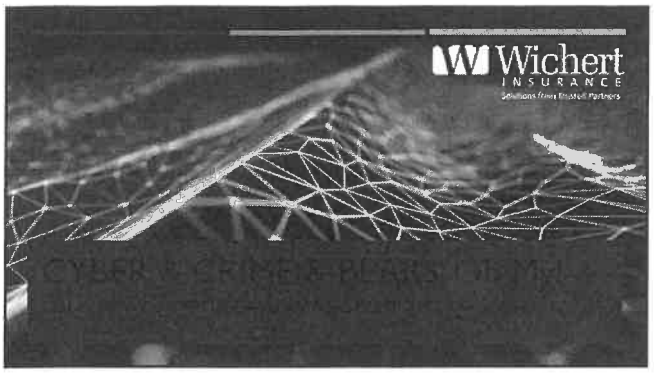
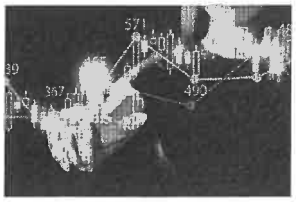


Implementation of any practices suggested is at your sole discretion. Wichert Insurance assumes no liability to any party for any damages arising out of or in connection with the information. This information is a summary of complex issues and may not cover all the finer points of a specific topic. Accordingly, this information is not intended to be legal advice, which should be obtained in consultation with an attorney.

Karl Dertnuth
Director
Information Technology

Richard A. Studenic
CPCU
Account Executive
Director of Sales



- Market Conditions
  - Depending on renewal
    - Nothing new
  - Since June
    - Open ports
    - Outdated software
    - Multi-factor authentication (MFA)

- Detailed Applications
  - IT Input
- Non Renewals
- Increased Prices
- Decreased Limits
- Deductibles/Retentions
- Attitude Toward Public Entities

Key Findings

Company Size

Small to Medium Enterprise (SME)

Categorized in this study as organizations with revenues $2 billion or less in annual revenue.

Large Company

Categorized in this study as organizations with $2 billion or more in annual revenue.

Costs

SMEs

Large Companies

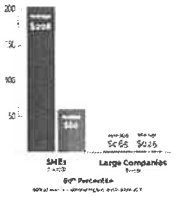
Business Interruption

SMEs

Records

Records Exposed

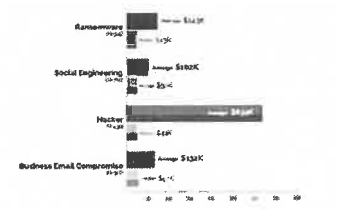
Per-Record Costs



Cause of Loss

Top 4 by Number of Claims

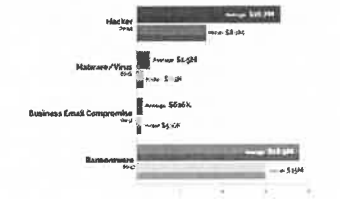
SMEs



Cause of Loss

Top 4 by Number of Claims

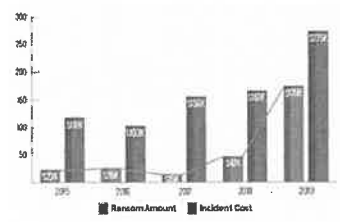
Large Companies



Focus on Ransomware

Leading Cause of Loss for SMEs

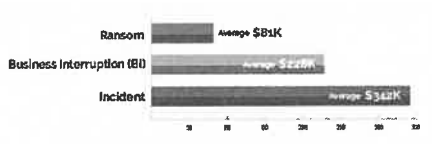
Average Costs by Year



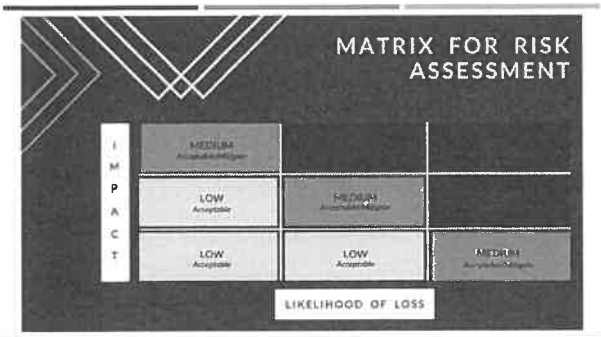
Focus on Ransomware

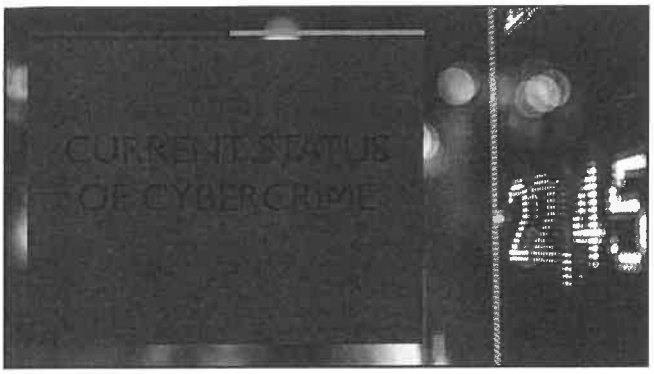
Leading Cause of Loss for SMEs

Ransomware that Included Business Interruption



MATRIX FOR RISK ASSESSMENT





[redacted]

- Atlanta
  - Discovered March 22, 2018
  - As of June, one-third of systems were still off-line
  - Estimated $9.5M recovery
  - Some legal documents and police dashcam videos were permanently deleted

[redacted]

- Baltimore
  - Discovered May 7, 2019
  - Weeks to recover
  - Lack of cyber insurance
  - Real estate market was impacted

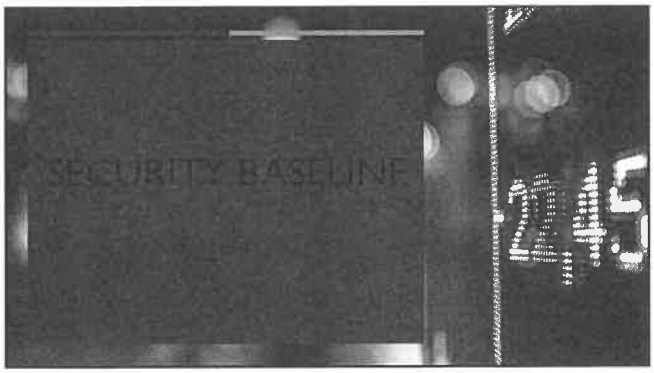
- New Bedford, MA
  - Discovered July 4, 2019
  - Ransomware demand of $5.3M
  - Only 4% of systems were affected
  - Recovered from backups after $400,000 ransom offer was rejected

- Social Engineering
  - Phishing/Vishing
  - Email Links/Attachments
  - Schemes of Confidence
  - Threats
- Web Browsing
- Network Vulnerabilities
- Malware
- Ransomware

- VPN
  - Sept. 28 joint release by NSA and CISA
  - Will insurance companies add requirements?
- Artificial Intelligence
  - Success/fail knowledge
  - Self-propagation tactics
  - Trusted system mimickery

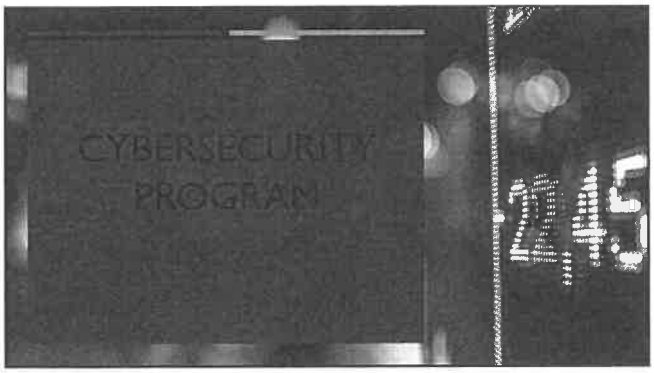
- Opportunity Cost
- System Downtime
- Reduced Efficiency
- Brand Damage or Loss of Trust
- IP Theft
- Incident Response Costs
- Outside Assistance
- Consultants
- Legal Assistance
- Cyber Risk Insurance
- Damage to Employee Morale

- Potential national security concerns
- Highest occurrence rate of insider attacks
- More likely to be publically disclosed or reported in media
- More concern regarding damage to brand and trust



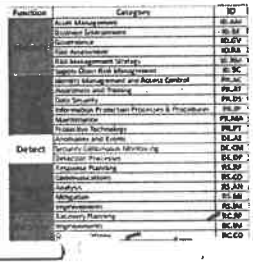
- Back to Paper!
  - Security is reduced to physical security only – No Cyber!
- Air Gapped Network
  - No Internet Access – (Either Direction)
  - Stuxnet – Iranian centrifuges were air gapped

- Strip Links and Attachments from Email
  - Will this break your world?!
- If these methods are untenable, what do we do?



- Is there a risk program that is required by statute?
- Not a checklist of procedures and technology
- Why is this important?

- NIST Cybersecurity Framework
  - https://nist.gov/cyberframework
- Investigate other frameworks that may be a better fit
  - ISO 27001 and ISO 27002
  - SOC2
  - NERC-CIP



VS

- Assets
  - Infrastructure
  - Network
  - Data
  - Privacy

VS

Where is the Balance?

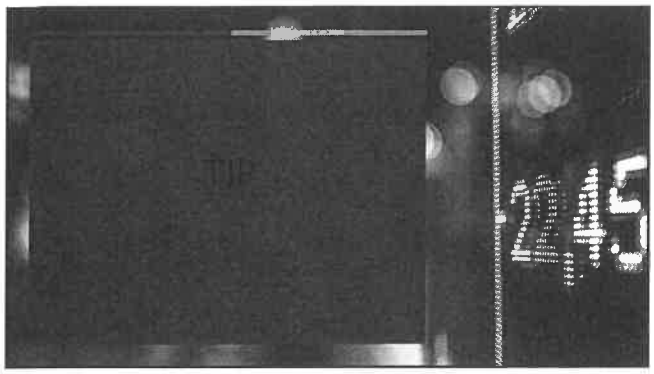
- Resources
  - Budget
  - Personnel
  - Services and Expertise
  - Technology
  - Insurance

- Who should drive this bus?
- Top-Down Approach
- Involve IT
- Why IT probably shouldn't drive the bus
  - May not see the whole picture
  - May have its own risk factors

- Is there a statutory mandate that we have a cybersecurity program?
- Do we base our program on a well-known framework?
- What factors do we consider and how do we measure and contrast them to acceptable risk levels?
- Is our plan cyclical?

- Do we employ the follow technologies?
  - Backups and are they available to hackers?
  - Antivirus and/or Endpoint Security
  - User education (bolster against social engineering)
  - Multifactor authentication
  - Network security (firewalls, endpoint authentication)

- Do we employee these services?
  - Secure DNS
  - Penetration testing
  - Security consulting
  - SEIM (security information and event management)



Karl Demuth < karl@wichert.com >
Subject: Check this out!
To: Tracy Combs

Hey Tracy,

Last years conference was grate. We have to register for the conference today so click http://www.ohioprima.org/general-education-conference.html to register ASAP.

Karl Demuth
Director of Information Technology
Wichert Insurance
1200 Graham Road
Cuyahoga Falls, OH 44224
Direct (330) 920-8641
Office (330) 929-8686
karl@wichert.com
www.wichert.com

CRIME	CYBER – 1ST PARTY	CYBER – 3RD PARTY
Computer Crime	Computer Fraud (Crime)	Network & Information Security/ Consultants & Incident Response
Funds Transfer Fraud	Funds Transfer Fraud (Crime)	Communications & Media/ Incident Response & Brand Damage
Employee Theft	Crisis Mgmt. Exp./ Outside Assistance & Consultants	Regulatory Defense/ Legal Asst. & Incident Response
Forgery Alteration	Security Breach Remediation/ Incident Response	
On Premises Theft	Computer Program Data Rest./ Downtime	
In Transit	E-Commerce Extension/ Payment to Bad Guys	
Counterfeit Money	Business Interruption/ Reduced Efficiency & Downtime	
Claim Expense		

- Claims Made Basis
- Retro Date
  - Full Prior Acts
  - Specified Date
- Continuity Date
- Other Insurance
  - Property/EDP
- Insurance Company
- Resources/Loss Control