

---

---

---

---


---

---

---

---

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 Dermuth**  
Director  
Operations Services  
kdermuth@wichert.com  
760.201.1147

**Responsibilities and Areas of Expertise**  
As Director of Operations Services, Karl is responsible for planning, managing and ongoing computer system and network, agency operations and process systems for all US carriers.

**Areas of Expertise**  
Karl is a member of the Senior Management Team and is responsible for the overall operations, support and success for the business. He has a strong background in the insurance industry and is a member of the Senior Management Team.

**Wichert Insurance**  
Wichert Insurance is a leading provider of leading technology solutions for the insurance industry. We are committed to providing the best service and support to our clients and partners. We are a leading provider of technology solutions for the insurance industry.



**Richard A. Stebbins**  
CEO  
Richard Stebbins  
Director of Sales  
rstebbins@wichert.com  
760.201.1147

**Responsibilities and Areas of Expertise**  
As CEO, Richard Stebbins is responsible for the overall operations, support and success for the business. He has a strong background in the insurance industry and is a member of the Senior Management Team.

**Wichert Insurance**  
Wichert Insurance is a leading provider of leading technology solutions for the insurance industry. We are committed to providing the best service and support to our clients and partners. We are a leading provider of technology solutions for the insurance industry.

---

---

---

---

---

---

---

---

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 • Outdated software  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

---

---

---

---

---

---

---

---

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

---

---

---

---

---

---

---

---

**Key Findings**  
**Company Size**

98%	Small to Medium Enterprises (SME)	Average Size: \$92M
2%	Large Companies	Average Size: \$6B

**Small to Medium Enterprise (SME)**  
 Categorized in this study as organizations with annual revenue of less than \$100 million.

**Large Company**  
 Categorized in this study as organizations with \$2 billion or more in annual revenue.

---

---

---

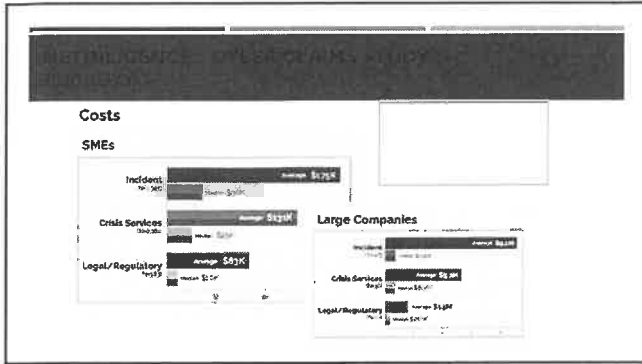
---

---

---

---

---




---

---

---

---

---

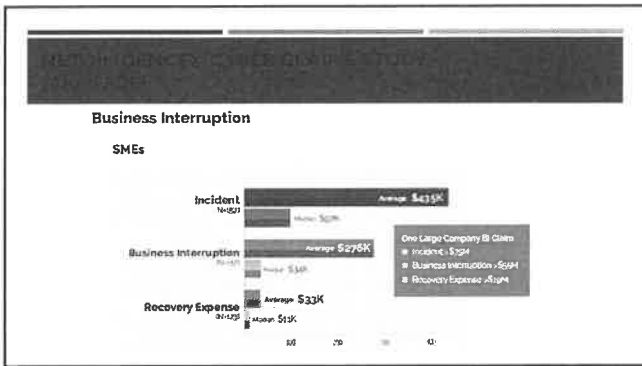
---

---

---

---

---




---

---

---

---

---

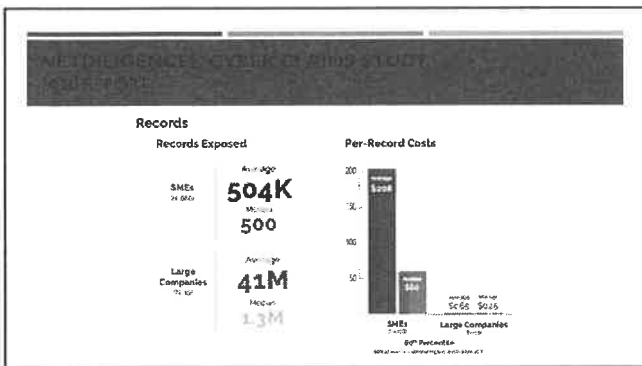
---

---

---

---

---




---

---

---

---

---

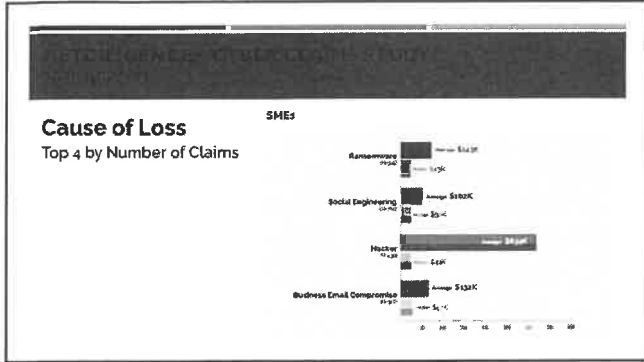
---

---

---

---

---



---

---

---

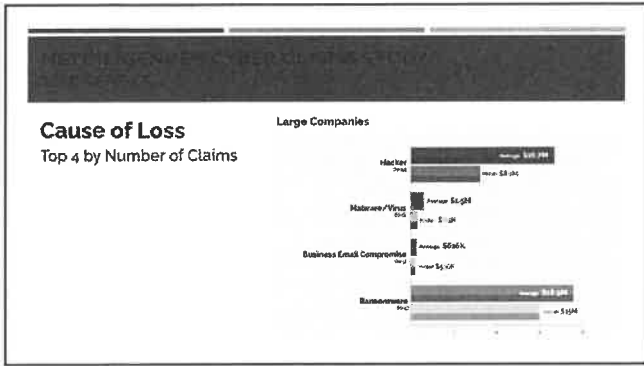
---

---

---

---

---



---

---

---

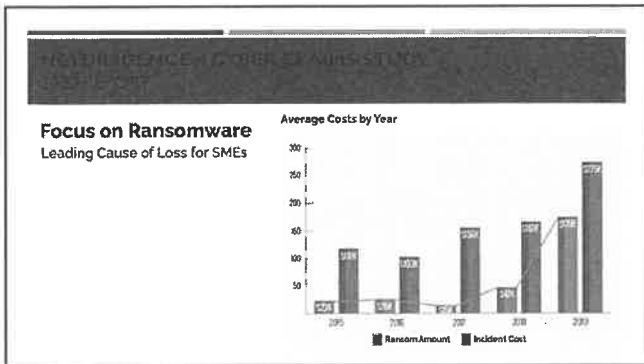
---

---

---

---

---



---

---

---

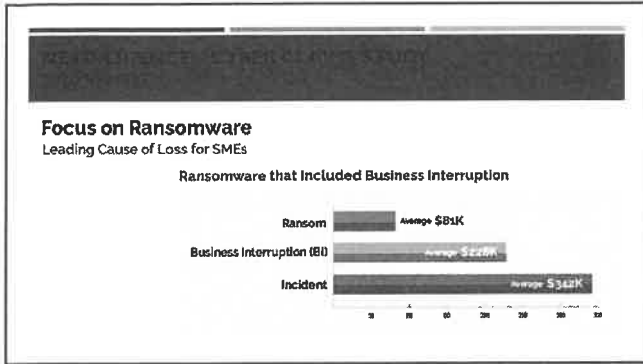
---

---

---

---

---



---

---

---

---

---

---

---

---



---

---

---

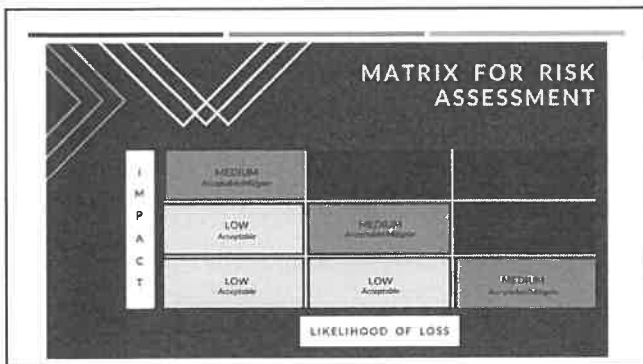
---

---

---

---

---



---

---

---

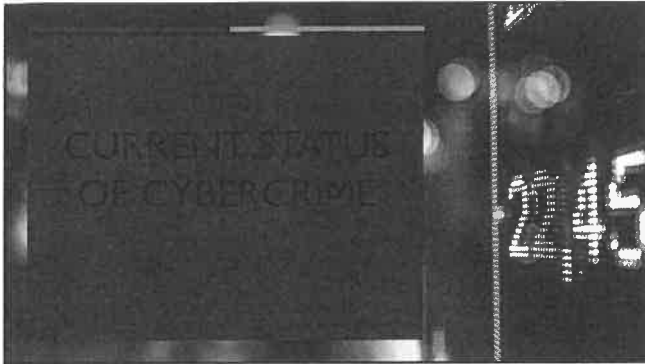
---

---

---

---

---



---

---

---

---

---


---

---

---

**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



---

---

---

---

---


---

---

---

**Baltimore**

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



---

---

---

---

---


---

---

---

**[Redacted]**

- 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



---

---

---

---

---

---

---

---

**[Redacted]**

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

---

---

---

---

---


---

---

---

**[Redacted]**

- 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

---

---

---

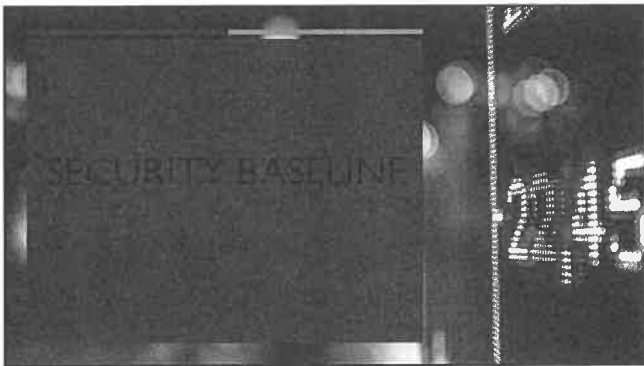
---

---

---

---

---



---

---

---

---

---

---

---

---



[Redacted]

- 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

---

---

---

---

---

---

---

---

[Redacted]

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

---

---

---

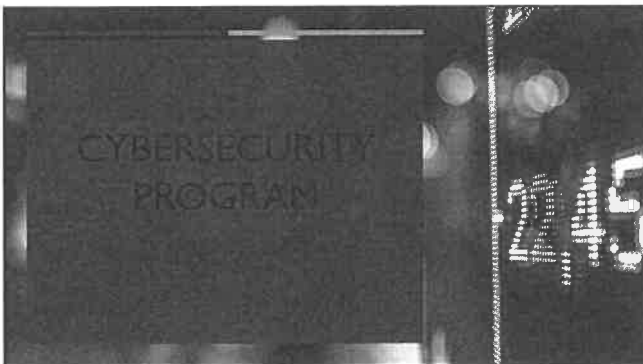
---

---

---

---

---



---

---

---

---

---

---


---

---

➤ 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

Function	Category	ID
Identify	Asset Management	IA-101
	Business System	IA-102
	Configuration	IA-103
	User Authentication	IA-104
	Risk Management Strategy	IR-101
	Security Classification and Access Control	IR-102
	Asset Protection and Training	IR-103
	Data Security	IR-104
	Information Protection Policies & Procedures	IR-105
	Maintenance	IR-106
Protect	System Security	PR-101
	Information and Events	PR-102
	Security Classification Information (SCI)	PR-103
	Security Plans	PR-104
	Language Planning	PR-105
	Communication	PR-106
	Language	PR-107
	Management	PR-108
	Language	PR-109
	Language	PR-110
Detect	Security Classification Information (SCI)	DC-101
	Security Plans	DC-102
	Language Planning	DC-103
	Communication	DC-104
	Language	DC-105
	Management	DC-106
	Language	DC-107
	Language	DC-108
	Language	DC-109
	Language	DC-110

---

---

---

---

---

---

---

---

VS

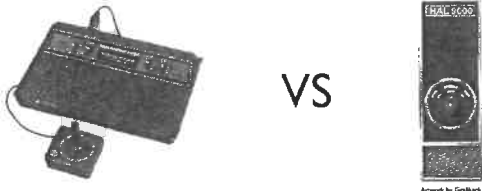


Image by Eric Aron

Image by Gellert1  
<https://commons.wikimedia.org/wiki/File:Smartphone>

---

---

---

---

---


---

---

---

**VS**

*Where is the Balance?*



- Assets
  - Infrastructure
  - Network
  - Data
  - Privacy
- 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



---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

[Redacted]

- 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?

---

---

---

---

---

---

---

[Redacted]

- 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)

---

---

---

---

---

---

---

[Redacted]

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

---

---

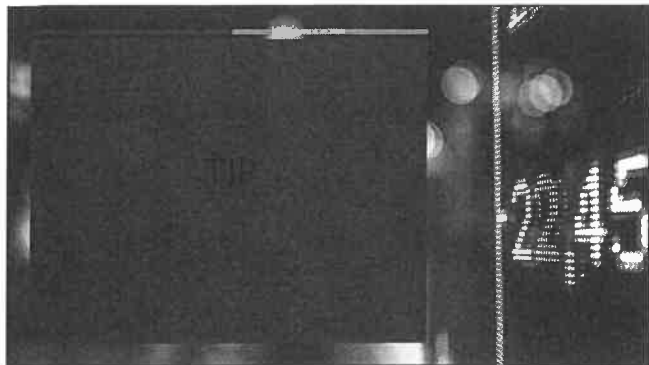
---

---

---

---

---



---

---

---

---

---

---

---


---

Karl Demuth <karl@wibert.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.ahioiprma.org/general-education-conference.html> to register ASAP.

Karl Demuth  
 Director of Information Technology  
 Wibert Insurance  
 1500 Graham Road  
 Cuyahoga Falls, OH 44224  
 Direct (330) 920-8641  
 Office (330) 929-8586  
[karl@wibert.com](mailto:karl@wibert.com)  
[www.wibert.com](http://www.wibert.com)



Wibert

---

---

---

---

---

---

---

---



---

---

---

---

---

---

---

---

CRIME	CYBER – 1 <sup>ST</sup> PARTY	CYBER – 3 <sup>RD</sup> 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
  - o Full Prior Acts
  - o Specified Date
- > Continuity Date
- > Other Insurance
  - o Property/EDP
- > Insurance Company
- > Resources/Loss Control

---

---

---

---

---

---

---

---

---

---

QUESTIONS?

THANK YOU

---

---

---

---

---

---

---

---

---

---