

Contemporary Cyber Risks/Threats & Prevention Strategies for the Energy Sector

For

The MEARIE Conference

June 21st, 2019



NetDiligence[®]

Dave Chatfield, VP/COO



CYBER RISK



READINESS



RESPONSE



About NetDiligence

18 years supporting the cyber liability risk mitigation needs of insurers and their clients

We provide access to our **eRiskHub®** cyber risk management portal for 80+ carriers, brokers, and risk pool organizations – and tens of thousands of their policyholders/clients (**including The MEARIE Group**).

We conduct **QuietAudit®** cyber risk assessments for organizations – and their vendors – of all sizes & sectors.

We build/host **Breach Plan Connect®** to help clients better organize and access key elements of their incident response plan capabilities.

We sponsor cyber risk **Cyber Risk Summit** conferences each year in Philadelphia, Santa Monica, Toronto, London & Bermuda.



CYBER RISK



READINESS



RESPONSE

Cyber Threat Sources Facing Energy Sector Organizations – 4 Typical Cases

“Traditional” Business Interruption Risks – Functional/unprovoked failures of servers/network appliances, applications, and/or network connectivity within the normal course of operations. Such failures can result in degraded or halted delivery of service and/or significantly impact the pace of internal business operations. Deferred maintenance, *force majeure* events, employee errors, and/or lack of component redundancy can represent typical root causes.

Privacy/Confidential Data Breach Risks (From Internal Causes) – Typically, employee errors or policy violations that result in sensitive information being transmitted outside of the organization. Client PII/PHI/PCI data is a usual case.

Malicious Acts Targeted Against Energy Production/Distribution Assets – Often referred to as exploits against Supervisory Control and Data Acquisition (**SCADA**) assets, such acts can be motivated by geopolitical control objectives, purposeful sabotage (e.g., former employees), random-directed chaos, or financial extortion.

Malicious Acts Targeted Against Internal Business/Consumer-Facing Operations – These are the more conventional types of exploits that many organizations (energy and non-energy alike) face in contemporary times. Prominent motives among these types of attacks are becoming predominantly financial in nature, although all of the above mentioned sources can apply as well.



CYBER RISK



READINESS



RESPONSE

Employee Error in Data Breach

eSecurity Planet

March 26, 2013

Texas Tech University Health Sciences Center Admits Data Breach

Approximately 700 patient billing statements were mistakenly sent to other patients' mailing addresses.

WSB-TV
ATLANTA 2

March 4, 2013

Confidential records found in Paulding Co. dumpster

Federal investigators are looking into a dumpster full of medical documents that Channel 2's Ross Cavitt found dumped outside an office complex in Hiram.

threat post

The Kaspersky Lab Security News Service January 17, 2013

'Terrific Employee' Fired After Losing USB Drive Containing Medical Records

NBCNEWS.com

12/13/2013

California Accidentally Posts 14,000 Social Security Numbers

The Boston Globe October 12, 2012 TD Bank misplaces tapes with data on 267,000 customers

SC
MAGAZINE
FOR IT SECURITY PROFESSIONALS

April 01, 2013

Doctor's stolen laptop found at pawn shop; data of 652 patients exposed



CYBER RISK



READINESS



RESPONSE

Common Methods/Types of Cyber Attacks

Distributed Denial-of-Service (DDoS) – Generation of excess traffic against a site so that “legitimate” traffic is denied. Simple, but effective if sufficient volume is generated. Financial extortion is the usual motive.

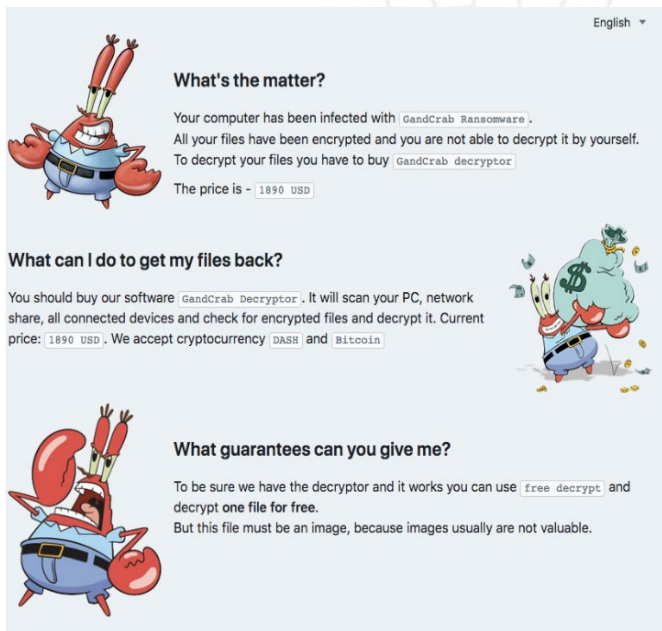
Ransomware – Someone, usually an employee, is enticed to click on a legitimate-looking email, but which instead encrypts all available files that the attack can reach, including system files (and even backups). Always extortion.

Phishing (or Spear-Phishing) – Convincing an employee to take incorrect action based upon instructions in a fake e-mail, often impersonating the CEO or other high-level manager. Often financially motivated – either through a request for wiring of funds or through the illicit theft/receipt of confidential data (client or proprietary).

“Rooting” or Other Type of System Takeover – Typically attempted by a higher-skilled attacker who can exploit known weaknesses in operating system, middle-ware, or application security on a given host or network component. Can be attempted in order to help form a “bot network”, but often more targeted as specific to you.



Ransomware Examples (And The Bad Guys' Obnoxious Sense of Humor)



English ▾

What's the matter?

Your computer has been infected with `GandCrab Ransomware`. All your files have been encrypted and you are not able to decrypt it by yourself. To decrypt your files you have to buy `GandCrab decryptor`.

The price is - `1890 USD`

What can I do to get my files back?

You should buy our software `GandCrab Decryptor`. It will scan your PC, network share, all connected devices and check for encrypted files and decrypt it. Current price: `1890 USD`. We accept cryptocurrency `DASH` and `Bitcoin`.

What guarantees can you give me?

To be sure we have the decryptor and it works you can use `free decrypt` and decrypt one file for free. But this file must be an image, because images usually are not valuable.

- The Ryuk (variant) locks all of the victim's network/ files — and in some cases, backup files, too — with encryption.
- The bad guys have the only decryption key and they demand Bitcoins to get it.
- Demands can be \$10k+; \$100k+ and even \$1mil+!

Those who missed the 72-hour deadline can also get their key, but the price jumps from two Bitcoins to 10. **At today's market value, that's \$77,000.**



Cryptolocker

Your personal files are encrypted!

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique public key RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able to restore files...**

To **obtain** the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount in another currency**.

Click «Next» to select the method of payment.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Private key will be destroyed on
13/10/2013
23:07

Time left
71 : 58 : 09

Next >>



CYBER RISK



READINESS



RESPONSE

A Note on Cybercrime (Increasing % of All Claims)

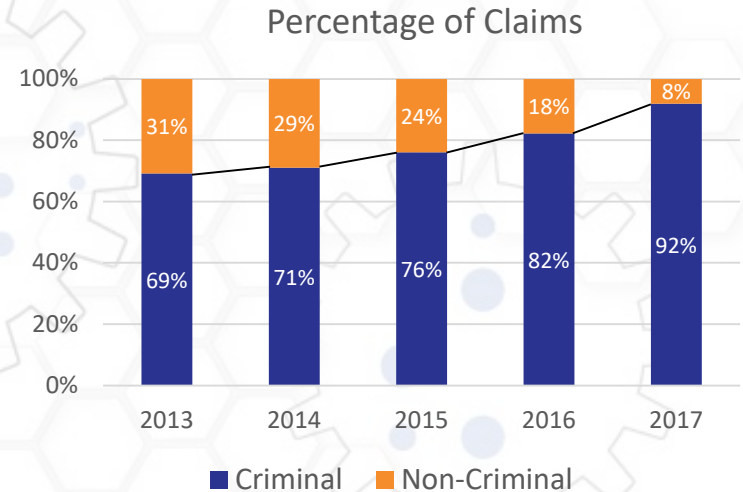
Insurance Industry Cybercrime Task Force (IICTF), sponsored by NetDiligence®

■ Ransomware demands explode in 2018

- Demands of \$250K-\$500K (nonexistent 6 months ago) now a weekly occurrence (Kivu)
- Top ransomware payouts began to exceed \$1M, dwarfing the previous max of \$17K (Chubb)

■ Top cybercrime-related causes

- Ransomware – 31%
- Phishing/BEC/Social Engineering – 24%
- Hacking – 19%
- Malware/Virus – 11%



CYBER RISK



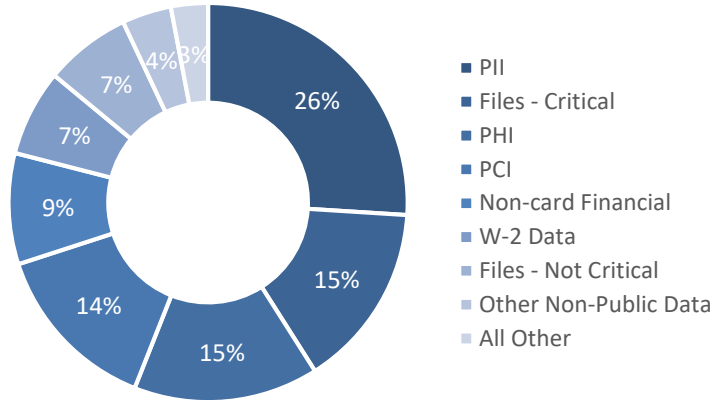
READINESS



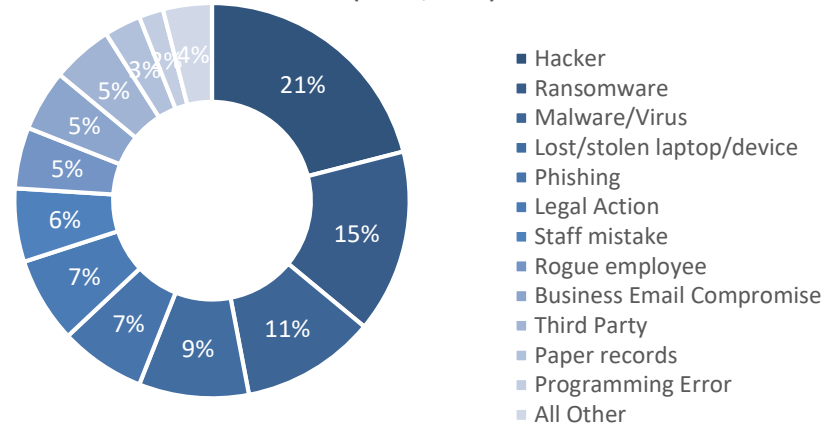
RESPONSE

NetDiligence® 2018 Cyber Claims Study (Summary Points)

% of Claims by Type of Data: 2013-2017
(N=1,201)



% of Claims by Cause of Loss: 2013-2017
(N=1,201)



CYBER RISK



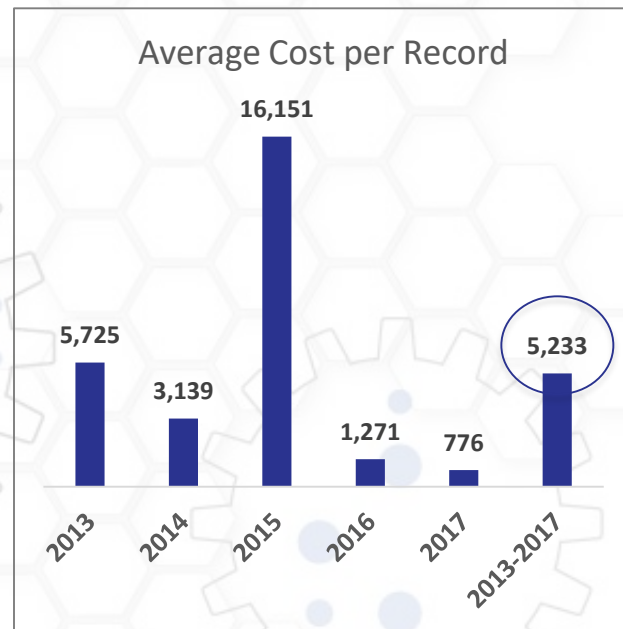
READINESS



RESPONSE

NetDiligence® 2018 Cyber Claims Study

- Claims Submitted 1,201
- Per-Breach Costs (N=1,194)
 - 5-Year Average \$603.9K
 - 2017 1-Year Average \$603.7K
 - 2017 1-Year Average – Large Co. \$24.6M
(median \$17.2M)
- Per-Record Costs (N=1,194)
 - 5-Year Average \$5.2K
(median \$43)
 - Cost Range \$0.001-\$1.6M



NetDiligence® 2018 Cyber Claims Study

■ Crisis Services

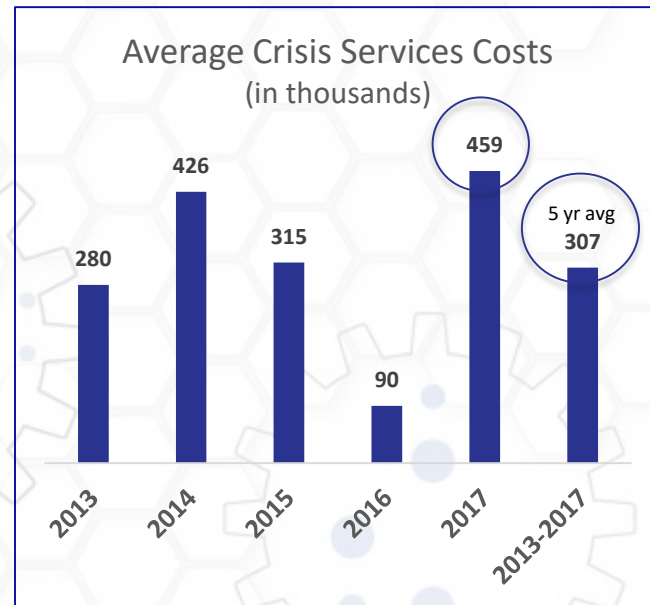
(forensics, legal counsel, notification, ID/credit monitoring, etc.)

- 5-Year Average **\$307K**
- 2017 1-Year Average **\$459K**

■ Legal Costs – 5-Year Averages

(defense & settlement)

- Legal Defense **\$106K**
- Regulatory Defense **\$514K**
- Settlement **\$224K**



NetDiligence® 2018 Cyber Claims Study

Business Interruption & Other “Record-less” Claims – All Causes of Loss

- Breach Recovery Expense*
 - 5-Year Average Cost (N=34) \$2.3M
 - 2017 1-Year Average (N=7) \$42K
- Business Interruption/Revenue Loss**
 - 5-Year Average Cost (N=21) \$1.3M

Top 10 Causes

Cause of Loss	CountOfCase
Ransomware	160
Hacker	61
Legal Action	56
Malware/Virus	46
Lost/stolen laptop/device	29
Phishing	29
Business Email Compromise	26
Denial of Service	18
Rogue employee	16
Programming Error	9

Footnotes

* BRE: expense items include: crisis services to include - data recovery/restoration, backups, data recreation (if backup fails), and offsite storage failure recoup

** BI Loss with DDoS Focus: a few very large cases drive 5 yr avg loss to \$6.8M. A few of the largest claims in the dataset included BI.



CYBER RISK



READINESS



RESPONSE

De-Identified Energy Sector Claims (From 2018 Report)

The following table from our annual Cyber Claims Study (2018) shows a handful of insurer-reported cyber claims for the energy sector for the past few years – including the carrier-paid amounts client losses:

Scenario ID	Country	Business Sector	Revenue Size	Type of Data	Cause of Loss	Total Cost
1928	US	Energy	Nano-Revenue (<\$50M)	User Credentials	Ransomware	\$32,622
1954	US	Energy	Micro-Revenue (\$50M-\$300M)	Unknown	Ransomware	\$10,000
2182	US	Energy	Unknown	Files - Critical	Hacker	\$152,884
2214	US	Energy	Micro-Revenue (\$50M-\$300M)	Files - Critical	Ransomware	\$131,942
2338	US	Energy	Nano-Revenue (<\$50M)	Files - Critical	Malware/Virus	\$45,059
2440	US	Energy	Nano-Revenue (<\$50M)	Files - Critical	Ransomware	\$32,621
2554	US	Energy	Micro-Revenue (\$50M-\$300M)	Files - Critical	Ransomware	\$11,017



CYBER RISK



READINESS



RESPONSE

Proactive Suggestions for Energy Sector Organizations

Perform a **Cyber Risk Assessment** (evaluating policies and supporting practices/procedures)

For particularly sensitive (e.g., SCADA) environments, perform a **Penetration Test**

Develop and operationalize a **Data Breach Incident Response Plan**

- Bolster your IRP... Self-help with outside experts
- Tiger Team experts
 - Breach Coach® (legal expert)
 - Computer Forensics (triage and establish the facts who, what, when, where & how)
 - Notification & Call Center
 - Credit & ID Monitoring

Conduct **Training** (especially anti-phishing) regularly for employees and vendors

Access **Available Services Provided by MEARIE (e.g., eRiskHub® Subscription)**

Utilize **Government-Provided & Third-Party Resources (e.g. Public Safety Canada)**



CYBER RISK



READINESS



RESPONSE

Proactive Technical/Process Suggestions for Energy Sector Organizations

Implement and manage a **Multi-Layered Network/Systems Security Architecture** that detects and deters bad-actor attempts to compromise sensitive systems (e.g., SCADA, customer billing, engineering diagrams, etc.). Some examples:

- Multiple firewalls, including segregation between business & energy generation
- Use of multiple-factor authentication (“MFA” or “2FA”) on privileged/critical systems
- Intrusion detection/prevention systems (“IDS/IPS”) to detect illicit usage attempts/patterns
- Periodic re-validation of user accounts on network (Active Directory) and application platforms

Ensure that all **Operating Systems and Applications are Kept Updated** to the Latest Available Version Levels/Patches.

- If official vendor-support has ceased – also known as End-of-Life – this is a major red flag.

Keep **Anti-Virus, Anti-Spam, and Other Security Protection Subscriptions Current**.



CYBER RISK



READINESS

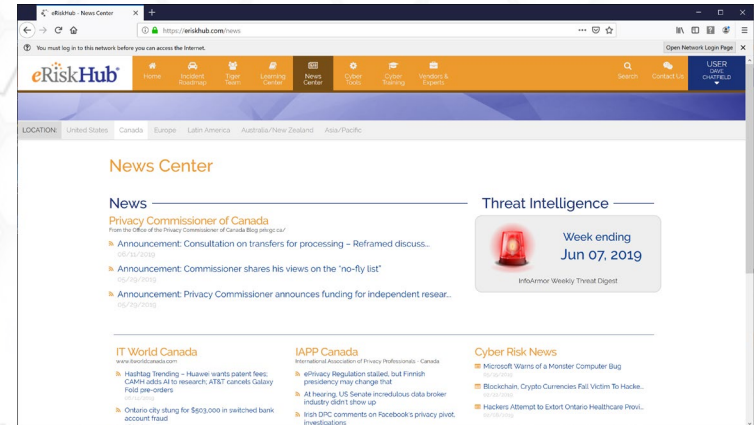


RESPONSE

eRiskHub® Unique Features in Your MEARIE Subscription



- Canadian News on Privacy & Information Security
- Proprietary Risk Tools:
 - Free Online Security Assessment (scorecard)
 - Free Security Policy library
 - Free use of unique research tools
 - Cyber claims paid & causes
 - Data breach cost calculator
 - Fines & penalties
 - Cause of loss



Access the eRiskHub through the mearie.ca – login with your regular account.



CYBER RISK



READINESS



RESPONSE

Canadian Energy Sector Cyber Risk Resource Examples

- Exceptional cyber security resource from Public Safety Canada:
 - <https://www.publicsafety.gc.ca/cnt/rsracs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx>
 - Provides strategic approach
 - Provides numerous additional resource contacts
- Canadian Advanced Technology Alliance
 - <https://www.itworldcanada.com/article/cata-report-on-critical-infrastructure-to-wake-smes-about-cyber-threats/412594>
 - SME-targeted report in progress that aims to explore risks associated with SCADA and Internet-connected Control Systems (ICSs); anticipated mid-2019.

 Public Safety
Canada

BUILDING A SAFE AND RESILIENT CANADA



Canada



CYBER RISK



READINESS



RESPONSE

NetDiligence®

eRiskHub®

QuietAudit®

BreachCoach®
Cyber Portal

BreachPlan
Connect®

Thank you!

Dave Chatfield
NetDiligence®

Dave.Chatfield@NetDiligence.com

954-684-9190



CYBER RISK



READINESS



RESPONSE