Cybersecurity For Municipalities

CML's 93rd Annual Conference
June 16 – 19, 2015
Breckenridge, Colorado

The contents of this presentation reflect the view of the presenter, not of CML.

Panelists

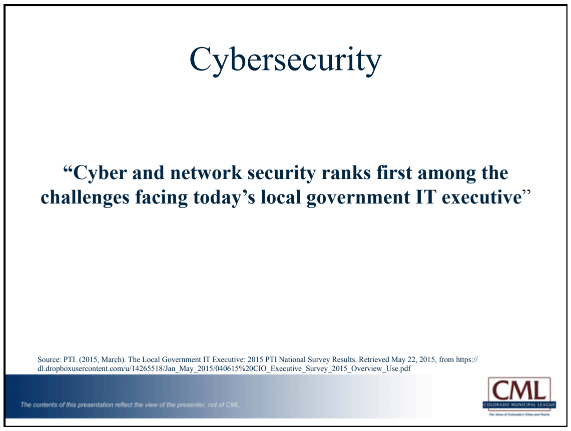
Inga Goddijn
Executive Vice President
Managing Director of Insurance Services
Risk Based Security

Paul Nelson
Chief Architect
AppliedTrust

Jeffrey A. Wells
City Manager
City of Fort Morgan

Ken C. Price
CML Information Technology Section Chair
Information Services Director
City of Littleton

The contents of this presentation reflect the view of the presenter, not of CML.

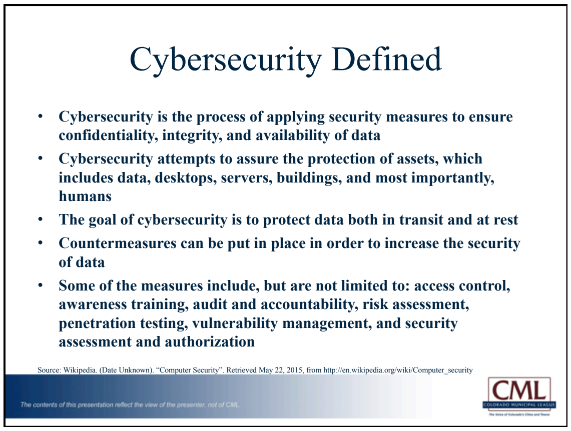


Cybersecurity

"Cyber and network security ranks first among the challenges facing today's local government IT executive"

Source: PTI. (2015, March). The Local Government IT Executive: 2015 PTI National Survey Results. Retrieved May 22, 2015, from https://dl.dropboxusercontent.com/u/14265518/Jan_May_2015/040615%20CIO_Executive_Survey_2015_Overview_Use.pdf

The contents of this presentation reflect the view of the presenter, not of CML.

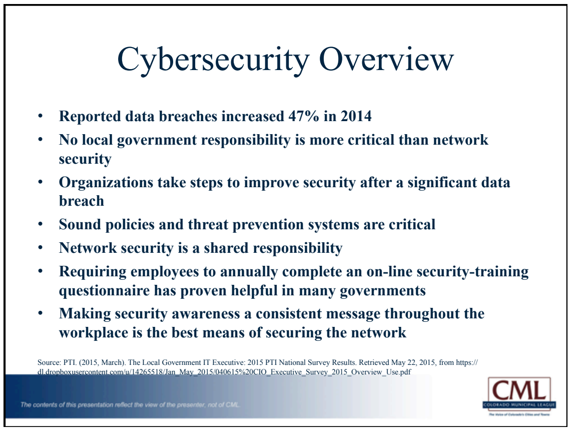


Cybersecurity Defined

- **Cybersecurity is the process of applying security measures to ensure confidentiality, integrity, and availability of data**
- **Cybersecurity attempts to assure the protection of assets, which includes data, desktops, servers, buildings, and most importantly, humans**
- **The goal of cybersecurity is to protect data both in transit and at rest**
- **Countermeasures can be put in place in order to increase the security of data**
- **Some of the measures include, but are not limited to: access control, awareness training, audit and accountability, risk assessment, penetration testing, vulnerability management, and security assessment and authorization**

Source: Wikipedia. (Date Unknown). "Computer Security". Retrieved May 22, 2015, from http://en.wikipedia.org/wiki/Computer_security

The contents of this presentation reflect the view of the presenter, not of CML.

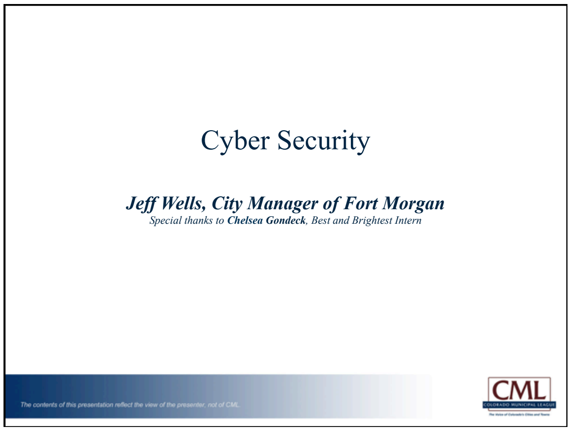


Cybersecurity Overview

- **Reported data breaches increased 47% in 2014**
- **No local government responsibility is more critical than network security**
- **Organizations take steps to improve security after a significant data breach**
- **Sound policies and threat prevention systems are critical**
- **Network security is a shared responsibility**
- **Requiring employees to annually complete an on-line security-training questionnaire has proven helpful in many governments**
- **Making security awareness a consistent message throughout the workplace is the best means of securing the network**

Source: PTI. (2015, March). The Local Government IT Executive: 2015 PTI National Survey Results. Retrieved May 22, 2015, from https://dl.dropboxusercontent.com/u/14265518/Jan_May_2015/040615%20CIO_Executive_Survey_2015_Overview_Use.pdf

The contents of this presentation reflect the view of the presenter, not of CML.

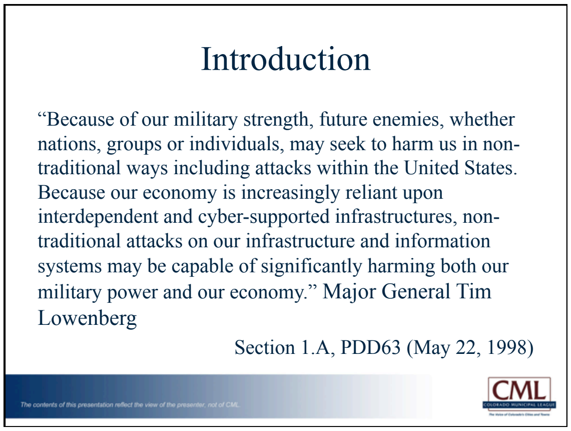


Cyber Security

Jeff Wells, City Manager of Fort Morgan

Special thanks to ***Chelsea Gondeck****, Best and Brightest Intern*

The contents of this presentation reflect the view of the presenter, not of CML.

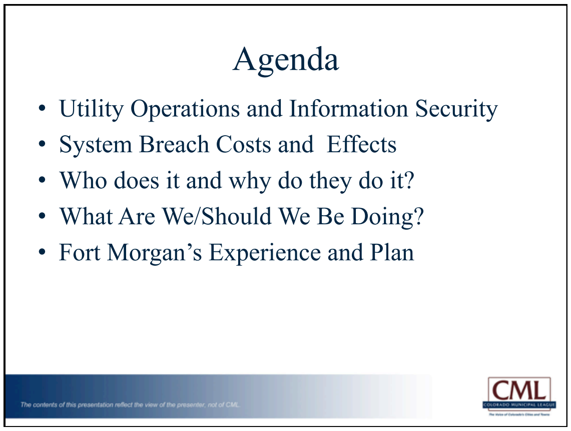


Introduction

"Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber-supported infrastructures, non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy." Major General Tim Lowenberg

Section 1.A, PDD63 (May 22, 1998)

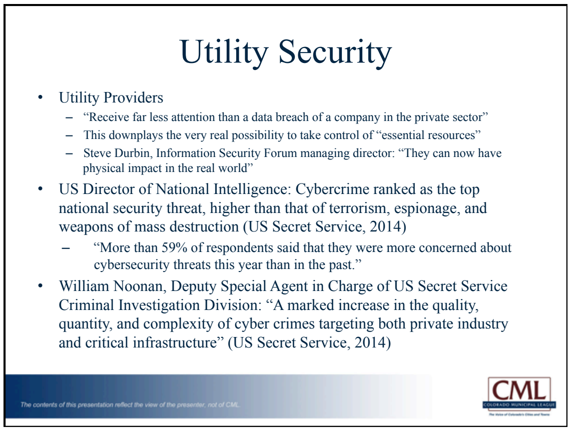
The contents of this presentation reflect the view of the presenter, not of CML



Agenda

- Utility Operations and Information Security
- System Breach Costs and Effects
- Who does it and why do they do it?
- What Are We/Should We Be Doing?
- Fort Morgan's Experience and Plan

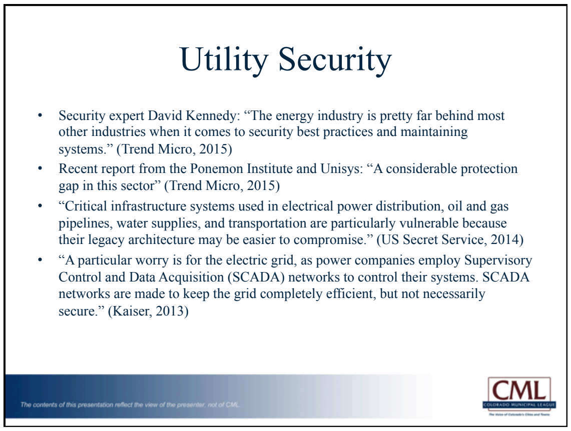
The contents of this presentation reflect the view of the presenter, not of CML



Utility Security

- Utility Providers
  - "Receive far less attention than a data breach of a company in the private sector"
  - This downplays the very real possibility to take control of "essential resources"
  - Steve Durbin, Information Security Forum managing director: "They can now have physical impact in the real world"
- US Director of National Intelligence: Cybercrime ranked as the top national security threat, higher than that of terrorism, espionage, and weapons of mass destruction (US Secret Service, 2014)
  - "More than 59% of respondents said that they were more concerned about cybersecurity threats this year than in the past."
- William Noonan, Deputy Special Agent in Charge of US Secret Service Criminal Investigation Division: "A marked increase in the quality, quantity, and complexity of cyber crimes targeting both private industry and critical infrastructure" (US Secret Service, 2014)

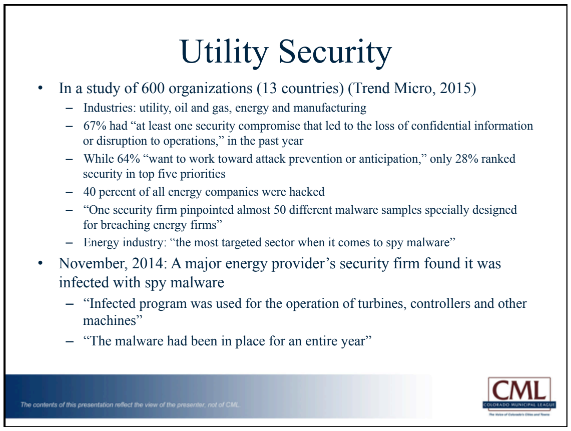
The contents of this presentation reflect the view of the presenter, not of CML



Utility Security

- Security expert David Kennedy: "The energy industry is pretty far behind most other industries when it comes to security best practices and maintaining systems." (Trend Micro, 2015)
- Recent report from the Ponemon Institute and Unisys: "A considerable protection gap in this sector" (Trend Micro, 2015)
- "Critical infrastructure systems used in electrical power distribution, oil and gas pipelines, water supplies, and transportation are particularly vulnerable because their legacy architecture may be easier to compromise." (US Secret Service, 2014)
- "A particular worry is for the electric grid, as power companies employ Supervisory Control and Data Acquisition (SCADA) networks to control their systems. SCADA networks are made to keep the grid completely efficient, but not necessarily secure." (Kaiser, 2013)

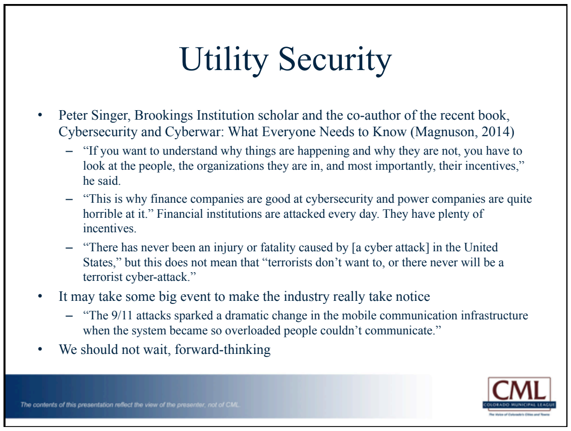
The contents of this presentation reflect the view of the presenter, not of CML



Utility Security

- In a study of 600 organizations (13 countries) (Trend Micro, 2015)
  - Industries: utility, oil and gas, energy and manufacturing
  - 67% had "at least one security compromise that led to the loss of confidential information or disruption to operations," in the past year
  - While 64% "want to work toward attack prevention or anticipation," only 28% ranked security in top five priorities
  - 40 percent of all energy companies were hacked
  - "One security firm pinpointed almost 50 different malware samples specially designed for breaching energy firms"
  - Energy industry: "the most targeted sector when it comes to spy malware"
- November, 2014: A major energy provider's security firm found it was infected with spy malware
  - "Infected program was used for the operation of turbines, controllers and other machines"
  - "The malware had been in place for an entire year"

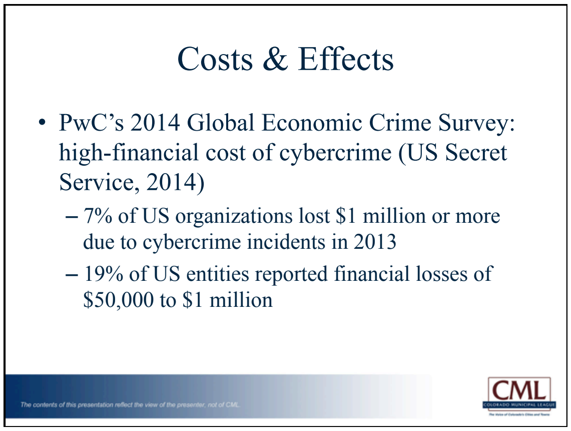
The contents of this presentation reflect the view of the presenter, not of CML



Utility Security

- Peter Singer, Brookings Institution scholar and the co-author of the recent book, Cybersecurity and Cyberwar: What Everyone Needs to Know (Magnuson, 2014)
  - "If you want to understand why things are happening and why they are not, you have to look at the people, the organizations they are in, and most importantly, their incentives," he said.
  - "This is why finance companies are good at cybersecurity and power companies are quite horrible at it." Financial institutions are attacked every day. They have plenty of incentives.
  - "There has never been an injury or fatality caused by [a cyber attack] in the United States," but this does not mean that "terrorists don't want to, or there never will be a terrorist cyber-attack."
- It may take some big event to make the industry really take notice
  - "The 9/11 attacks sparked a dramatic change in the mobile communication infrastructure when the system became so overloaded people couldn't communicate."
- We should not wait, forward-thinking

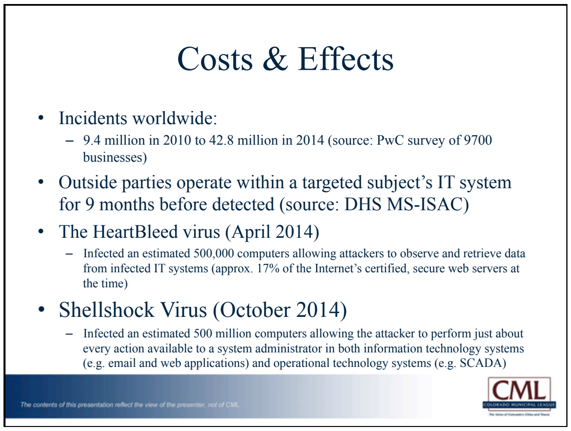
The contents of this presentation reflect the view of the presenter, not of CML



Costs & Effects

- PwC's 2014 Global Economic Crime Survey: high-financial cost of cybercrime (US Secret Service, 2014)
  - 7% of US organizations lost $1 million or more due to cybercrime incidents in 2013
  - 19% of US entities reported financial losses of $50,000 to $1 million

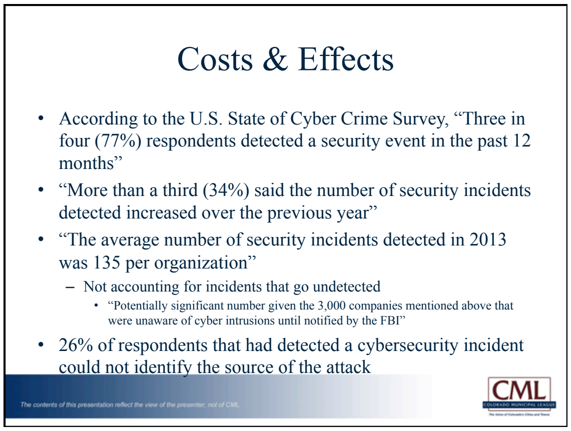
The contents of this presentation reflect the view of the presenter, not of CML.



Costs & Effects

- Incidents worldwide:
  - 9.4 million in 2010 to 42.8 million in 2014 (source: PwC survey of 9700 businesses)
- Outside parties operate within a targeted subject's IT system for 9 months before detected (source: DHS MS-ISAC)
- The HeartBleed virus (April 2014)
  - Infected an estimated 500,000 computers allowing attackers to observe and retrieve data from infected IT systems (approx. 17% of the Internet's certified, secure web servers at the time)
- Shellshock Virus (October 2014)
  - Infected an estimated 500 million computers allowing the attacker to perform just about every action available to a system administrator in both information technology systems (e.g. email and web applications) and operational technology systems (e.g. SCADA)

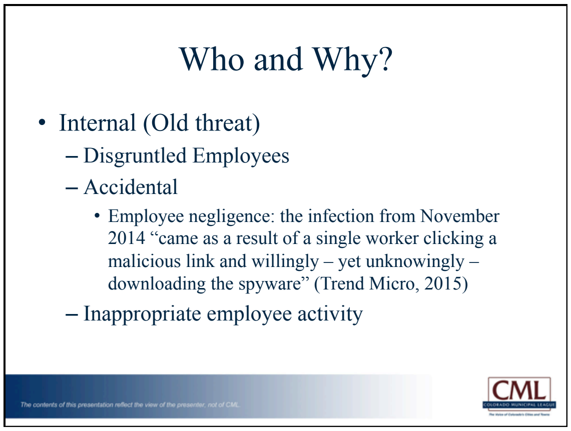
The contents of this presentation reflect the view of the presenter, not of CML.



Costs & Effects

- According to the U.S. State of Cyber Crime Survey, "Three in four (77%) respondents detected a security event in the past 12 months"
- "More than a third (34%) said the number of security incidents detected increased over the previous year"
- "The average number of security incidents detected in 2013 was 135 per organization"
  - Not accounting for incidents that go undetected
    - "Potentially significant number given the 3,000 companies mentioned above that were unaware of cyber intrusions until notified by the FBI"
- 26% of respondents that had detected a cybersecurity incident could not identify the source of the attack

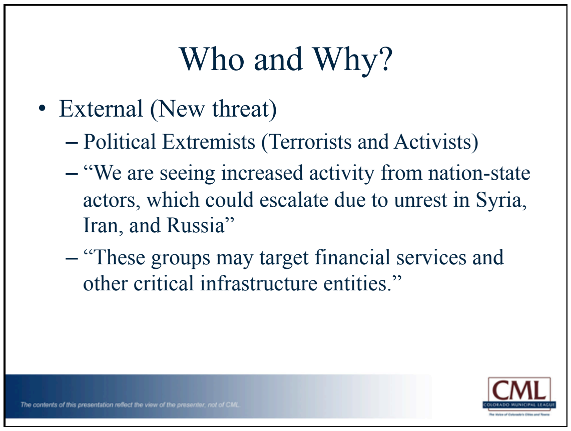
The contents of this presentation reflect the view of the presenter, not of CML.



Who and Why?

- Internal (Old threat)
  - Disgruntled Employees
  - Accidental
    - Employee negligence: the infection from November 2014 "came as a result of a single worker clicking a malicious link and willingly – yet unknowingly – downloading the spyware" (Trend Micro, 2015)
  - Inappropriate employee activity

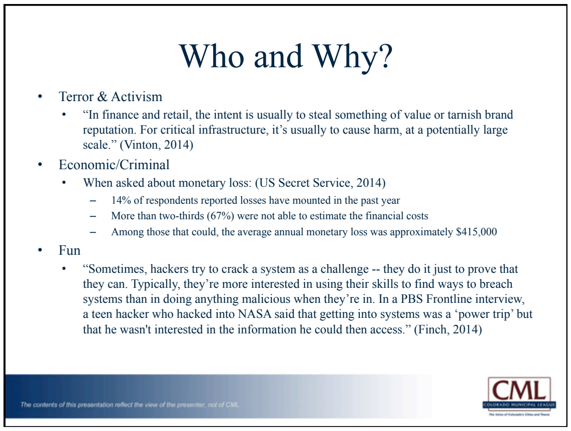
The contents of this presentation reflect the view of the presenter, not of CML.



Who and Why?

- External (New threat)
  - Political Extremists (Terrorists and Activists)
  - "We are seeing increased activity from nation-state actors, which could escalate due to unrest in Syria, Iran, and Russia"
  - "These groups may target financial services and other critical infrastructure entities."

The contents of this presentation reflect the view of the presenter, not of CML.



Who and Why?

- Terror & Activism
  - "In finance and retail, the intent is usually to steal something of value or tarnish brand reputation. For critical infrastructure, it's usually to cause harm, at a potentially large scale." (Vinton, 2014)
- Economic/Criminal
  - When asked about monetary loss: (US Secret Service, 2014)
    - 14% of respondents reported losses have mounted in the past year
    - More than two-thirds (67%) were not able to estimate the financial costs
    - Among those that could, the average annual monetary loss was approximately $415,000
- Fun
  - "Sometimes, hackers try to crack a system as a challenge -- they do it just to prove that they can. Typically, they're more interested in using their skills to find ways to breach systems than in doing anything malicious when they're in. In a PBS Frontline interview, a teen hacker who hacked into NASA said that getting into systems was a 'power trip' but that he wasn't interested in the information he could then access." (Finch, 2014)

The contents of this presentation reflect the view of the presenter, not of CML.

Who and Why?

What Are We/Should We Be Doing?

1. **Updated Software**
   - “Many industrial systems in the U.S. are still operating on outdated technology” (Trend Micro, 2015)
     - Some dating back to the 1970s
     - “Systems simply aren’t sophisticated enough to stand up to today’s hacking techniques”
   - “Cybersecurity programs of US organizations do not rival the persistence and technological prowess of their cyber adversaries.” (US Secret Service, 2014)
     - Lowenberg: “Prioritize installation of hardware and software upgrades to protect against reported vulnerabilities and emerging threats”

What Are We/Should We Be Doing?

2. **Training Employees**
   - 47% of attacks in the utilities industry came due to “negligence on the part of staff members”
   - “Despite these instances, a mere 6% percent of study respondents currently had training programs in place for their workers”
   - “Ensure that employees have the knowledge and ability to respond to threats and mitigate the damage of cybercriminal activities”
   - “42% of respondents said security education and awareness for new employees played a role in deterring a potential criminal, among the highest of all policies and technologies used for deterrence” (US Secret Service, 2014)

What Are We/Should We Be Doing?

3. **Collaboration, Partnership and Working Together**
   - Secretary of Homeland Security Jeh Johnson: “Cybersecurity is a shared responsibility” (US Secret Service, 2014)
   - “Everyone needs to work on this: Government officials and business leaders, security professionals, and utility owners and operators”
   - “The global risks and repercussions of cybercrime may seem overwhelming for any single organization,” but “there is strength in numbers”
   - “Private and public organizations are starting to band together to combat cybercrime and gain intelligence about current security threats and effective responses”

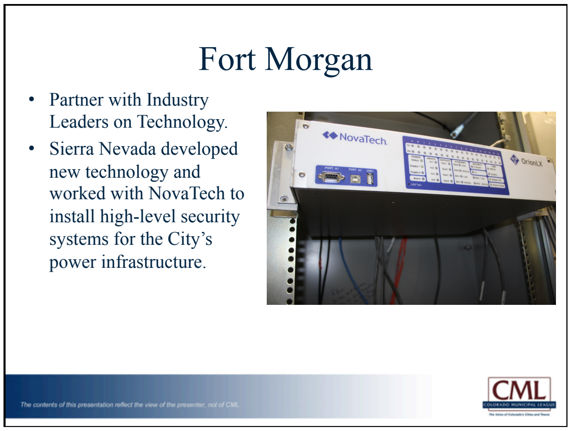
What Are We/Should We Be Doing?

4. **Conduct exercises:**
   - Examine organizations’ capability to prepare for, protect from, and respond to cyber attacks’ potential effects;
   - Exercise strategic decision making and interagency coordination of incident response(s) in accordance with national level policy and procedures;
   - Validate information sharing relationships and communications paths for collecting and disseminating cyber incident situational awareness, response and recovery information; and
   - Examine means and processes through which to share sensitive information across boundaries and sectors without compromising proprietary or national security interests.

- Department of Homeland Security’s biennial capstone cyber exercise

Fort Morgan’s Plan

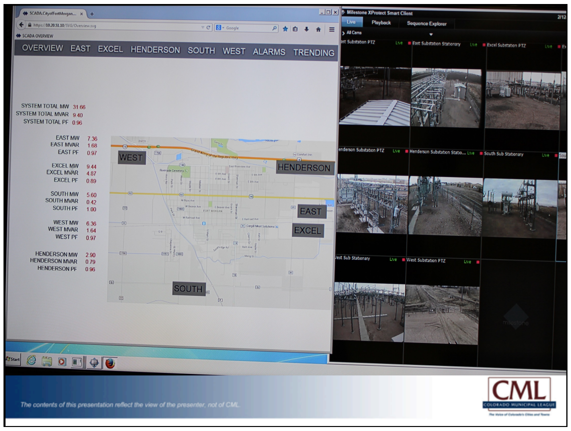
- Fort Morgan is implementing its plan in phases.
  - Phase I – Work with Employees to assess and address cyber threats
    - Social engineering awareness and employee training.
    - Establish best security practices and procedures.
    - Incorporate cyber security into annual emergency planning exercises.
    - Develop relationships with industry experts and peers.
    - Incorporate newest technology into networks.
  - Phase II – Electric Utility Security
  - Phase III – Water Utility Security
  - Phase IV – Remaining Utilities



Fort Morgan

- Partner with Industry Leaders on Technology.
- Sierra Nevada developed new technology and worked with NovaTech to install high-level security systems for the City's power infrastructure.

The contents of this presentation reflect the view of the presenter, not of CML.

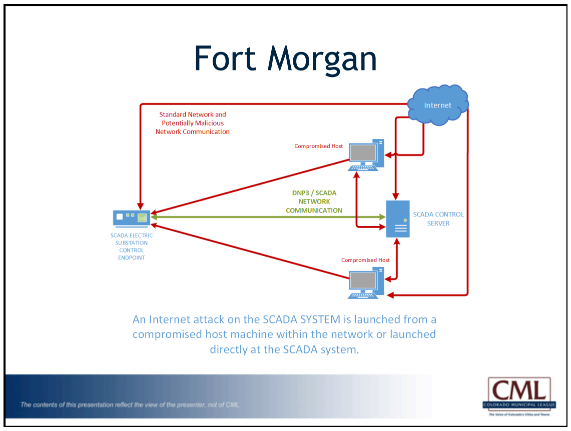


SCADA OVERVIEW

OVERVIEW EAST EXCEL HENDERSON SOUTH WEST ALARMS TRENDING

```
SYSTEM TOTAL MW    31.66
SYSTEM TOTAL MVAR   9.40
SYSTEM TOTAL PF     0.96

EAST MW       7.36
EAST MVAR     1.68
EAST PF       0.97

EXCEL MW      9.44
EXCEL MVAR    4.87
EXCEL PF      0.89

SOUTH MW      5.60
SOUTH MVAR    0.42
SOUTH PF      1.00

WEST MW       6.36
WEST MVAR     1.64
WEST PF       0.97

HENDERSON MW    2.90
HENDERSON MVAR  0.79
HENDERSON PF    0.96
```

The contents of this presentation reflect the view of the presenter, not of CML.

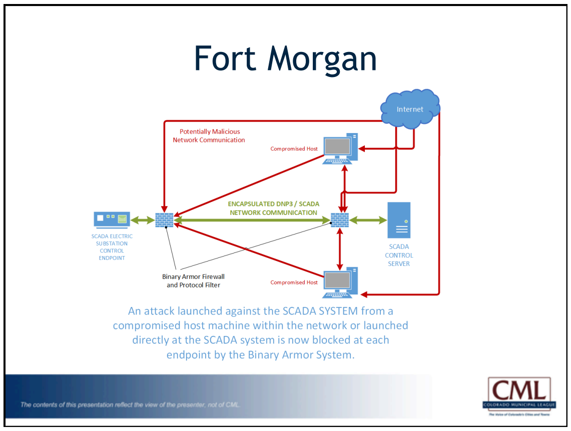


Fort Morgan

Internet
Standard Network and Potentially Malicious Network Communication
Compromised Host
DNP3 / SCADA NETWORK COMMUNICATION
SCADA CONTROL SERVER
SCADA ELECTRIC SUBSTATION CONTROL ENDPOINT
Compromised Host

An Internet attack on the SCADA SYSTEM is launched from a compromised host machine within the network or launched directly at the SCADA system.

The contents of this presentation reflect the view of the presenter, not of CML.



Fort Morgan

Internet
Potentially Malicious Network Communication
Compromised Host
ENCAPSULATED DNP3 / SCADA NETWORK COMMUNICATION
SCADA ELECTRIC SUBSTATION CONTROL ENDPOINT
SCADA CONTROL SERVER
Binary Armor Firewall and Protocol Filter
Compromised Host

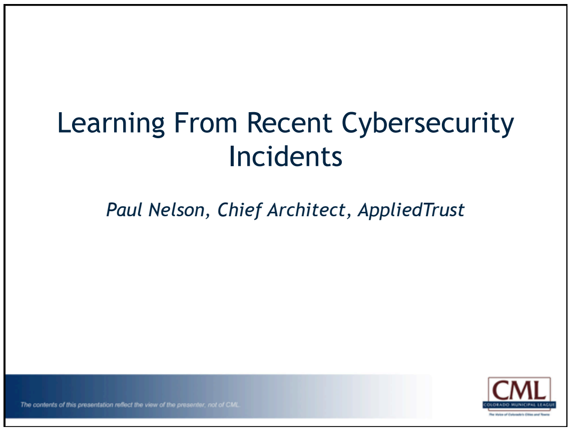
An attack launched against the SCADA SYSTEM from a compromised host machine within the network or launched directly at the SCADA system is now blocked at each endpoint by the Binary Armor System.

The contents of this presentation reflect the view of the presenter, not of CML.

Fort Morgan

- Lowenberg: "It is important to get this process started in small communities" because they can be the 'soft targets' that get used by larger terrorist groups to test their strategies and prepare for larger attacks.
- City Council were critical leaders in our experience as they provided policy and financial support to the plan.
- The plan promotes proactive preparation to ensure that the City is not a soft target.

The contents of this presentation reflect the view of the presenter, not of CML.



Learning From Recent Cybersecurity Incidents

Paul Nelson, Chief Architect, AppliedTrust

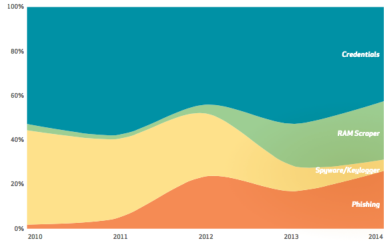
The contents of this presentation reflect the view of the presenter, not of CML.

Breach Notification - A National Issue

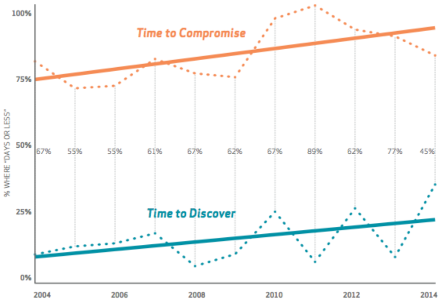
"We're introducing new legislation to create a single strong national standard so Americans know when their information has been stolen or misused. Right now almost every state has a different law on this and it's confusing for consumers and it's confusing for companies - and it's costly too, to have to comply with this patchwork of laws."

– *President Barack Obama, Remarks at the Federal Trade Commission, January 12, 2015*

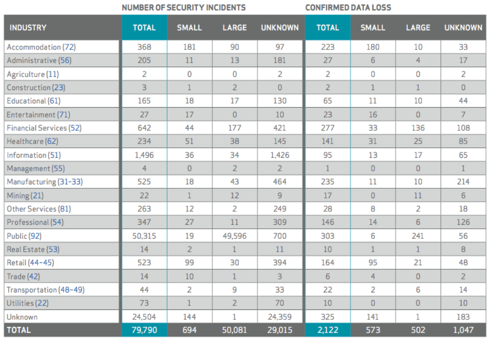
How Are Cybersecurity Attacks Evolving?



Source: 2015 Verizon Data Breach Investigation Report, atru.st/vdbir



Source: 2015 Verizon Data Breach Investigation Report, atru.st/vdbir



	NUMBER OF SECURITY INCIDENTS				CONFIRMED DATA LOSS			
INDUSTRY	TOTAL	SMALL	LARGE	UNKNOWN	TOTAL	SMALL	LARGE	UNKNOWN
Accommodation (72)	368	181	90	97	223	180	10	33
Administrative (56)	205	11	13	181	27	6	4	17
Agriculture (11)	2	0	0	2	2	0	0	2
Construction (23)	3	1	2	0	2	1	1	0
Educational (61)	165	18	17	130	65	11	10	44
Entertainment (71)	27	17	0	10	23	16	0	7
Financial Services (52)	642	44	177	421	277	33	136	108
Healthcare (62)	234	51	38	145	141	31	25	85
Information (51)	1,496	36	34	1,426	95	13	17	65
Management (55)	4	0	2	2	1	0	0	1
Manufacturing (31-33)	525	18	43	464	235	11	10	214
Mining (21)	22	1	12	9	17	0	11	6
Other Services (81)	263	12	2	249	28	8	2	18
Professional (54)	347	27	11	309	146	14	6	126
Public (92)	50,315	19	49,596	700	303	6	241	56
Real Estate (53)	14	2	1	11	10	1	1	8
Retail (44-45)	523	99	30	394	164	95	21	48
Trade (42)	14	10	1	3	6	4	0	2
Transportation (48-49)	44	2	9	33	22	2	6	14
Utilities (22)	73	1	2	70	10	0	0	10
Unknown	24,504	144	1	24,359	325	141	1	183
TOTAL	79,790	694	50,081	29,015	2,122	573	502	1,047

Source: 2015 Verizon Data Breach Investigation Report, atru.st/vdbir

Three real-world examples

- Public and private sector (nobody is safe!)
- Financial gain is usually the core intent:
  - Data theft (IP, PII, PHI, PANs/SAD, etc.)
  - Ransom scenarios (malware, DoS)
  - Direct financial gain
- Reputation impacts are understood in some cases (by attackers), but often secondary to $.
- This is not a name and shame – examples have been anonymized.

Case Study 1: Wire Transfer Complete!

- Detection: A staff member at Springfield Burns Power followed up with their supervisor who had requested they process an urgent wire transfer. By email.

```
From: Mr. Burns [mailto:cmburns@sprngfield-burns-power.com]
Sent: Friday, September 01, 2015 2:26 PM
To: W. Smithers
Subject: Wiring Instruction

Smithers,

Process a wire of $48,750 to the attached account information right away.
Code it to strategy and notify me once completed.

I'll send support later on.

C. M. Burns.
```

CREDIT: FIRST MIDDLE LAST
BANK NAME: <BANK>
BANK ADDRESS: <ADDRESS>
ACCOUNT NUMBER: <ACCOUNT NUMBER>
ROUTING NUMBER: <ROUTING NUMBER>

- Smithers first thought something was fishy when he called Mr. Burns to let him know the wire has been sent (phone, as opposed to email).

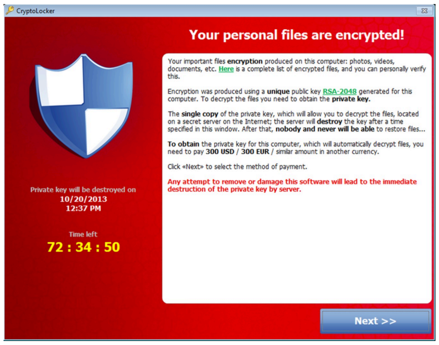
Anatomy of Attack

- Targeted phishing attack (spear phishing).
- Knew the names of financial contacts and roles (thank you LinkedIn!)
- Preyed on urgency/established personal relationship and management hierarchy.
- One last hurdle:

```
From: Mr. Burns [mailto:cmburns@sprngfield-burns-power.com]
```

Case Study 2: Ransomware

- Detection: Users began to have issues accessing files on a team share on a lightly used server.
- Multiple possible delivery vectors for first infection.
- The most well known version of this is the slightly more polished “cryptolocker”.
- Server taken offline, but large centralized share server was reported infected the next day.
- In total, 180,000 files, over 85GB of data were encrypted by multiple clients, no recovery options.



Your personal files are encrypted!

Private key will be destroyed on
10/20/2013
12:37 PM

Time left
72 : 34 : 50

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 the 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.

Like Wildfire

- Rapid vendor response for signature, but…
- <0.5% of clients were not adequately protected with AV.
- Rapid evolution of derivatives. Heuristic detection is only so good. Constant catch-up over a week.
- Defense in depth requires in-depth controls; known gaps mean real risk.
- Did I mention backups?

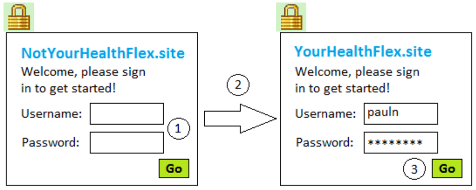
Road to Recovery

- Varying success (and horror) ransom stories.
- Client-side, we received no decrypt instructions.
- Backups?
- One less than beta-quality tool from an AV vendor (and rejected requests for bug fixes).
- 60+ hours of effort to code and use a quarantine extraction tool.
- ~90% of files/data recovered that were lost.
- External user CIFS access.

Case Study 3: Fraudulent HRA Portal

- Detection: Several users in a large organization did not receive their HRA reimbursements.
- A group of individuals received an email requesting annual verification of HRA details.
- Attackers built an imposter HRA site by scraping the real site. URLs were different, but so too is user sophistication/awareness…

The contents of this presentation reflect the view of the presenter, not of CML.



NotYourHealthFlex.site
Welcome, please sign in to get started!
Username:
Password:
Go

YourHealthFlex.site
Welcome, please sign in to get started!
Username: pauln
Password: ********
Go

- This is trivial to do if users don't check the domain name (but there's a padlock!)
- Any user concerns were quickly alleviated – they are directed to the real site.

The contents of this presentation reflect the view of the presenter, not of CML.

Anatomy of Attack

- Contrast this with the wire case, which relied heavily on non-private but presumed internal knowledge.
- Email was again the attack vector here, but other techniques could have been used.
- Credential grab and replay technique, allowing later modification of direct deposit HRA reimbursement details.

The contents of this presentation reflect the view of the presenter, not of CML.

Lessons & Thoughts

- Defense in depth – all layers/control points are important, beware the weakest link.
- Credentials are a target, and users are a target.
- With reasonable care and ongoing vigilance, technical controls can help reduce the risk of technical attacks.
- Edge DLP and SSL/TLS interception will become (necessarily) more prevalent.
- People are a *critical* part of the puzzle.

The contents of this presentation reflect the view of the presenter, not of CML.

The Soft, Gooey Center

- How much time have you dedicated to user awareness training?
- What is the quality, engagement level and effectiveness of your training program?
- Looking back on these attacks, people with legitimate access serve as the easiest target.
- Remember the defender-detection deficit.

The contents of this presentation reflect the view of the presenter, not of CML.

Improving Awareness

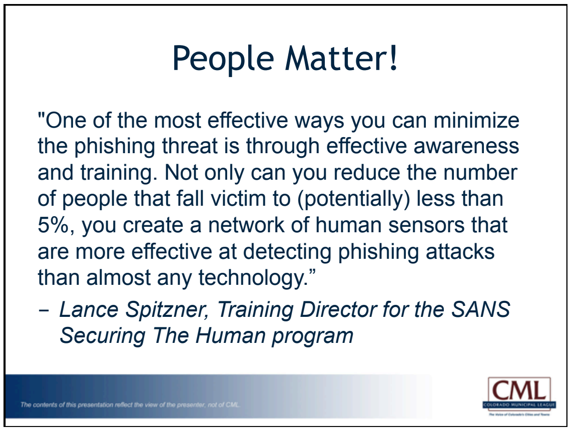
- What would you do if your firewall ignored rules a quarter of the time?
- Sending 10 emails yields a 90% chance one user will fall prey.
- Better filtering/edge detection.
- Think beyond just email to social engineering as well.
- Support a rapid response framework.
- Effort now or (much more) effort later.

23%
OF RECIPIENTS NOW OPEN PHISHING MESSAGES AND 11% CLICK ON ATTACHMENTS.

50%
NEARLY 50% OPEN E-MAILS AND CLICK ON PHISHING LINKS WITHIN THE FIRST HOUR.

Source: 2015 Verizon Data Breach Investigation Report, atru.st/vdbir

The contents of this presentation reflect the view of the presenter, not of CML.



People Matter!

"One of the most effective ways you can minimize the phishing threat is through effective awareness and training. Not only can you reduce the number of people that fall victim to (potentially) less than 5%, you create a network of human sensors that are more effective at detecting phishing attacks than almost any technology."

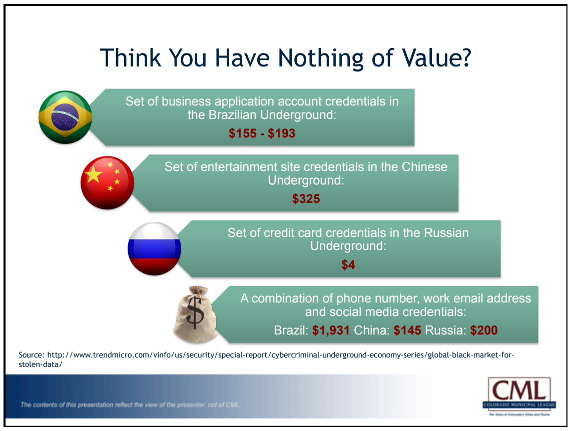
– *Lance Spitzner, Training Director for the SANS Securing The Human program*

The contents of this presentation reflect the view of the presenter, not of CML.

Cyber Security Insurance
What it is & Why we need it

Inga Goddijn, EVP & Managing Director of Insurance Services

The contents of this presentation reflect the view of the presenter, not of CML.



Think You Have Nothing of Value?

Set of business application account credentials in the Brazilian Underground:
$155 - $193

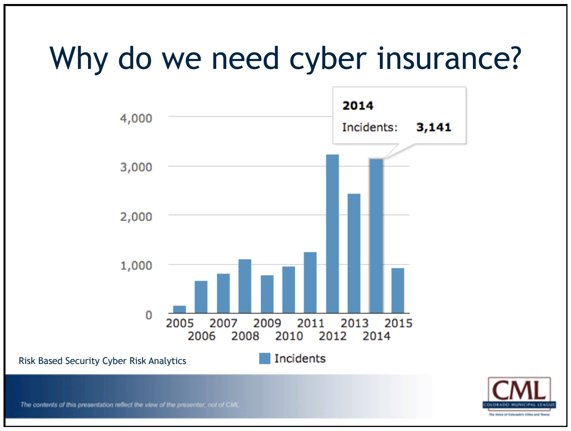
Set of entertainment site credentials in the Chinese Underground:
$325

Set of credit card credentials in the Russian Underground:
$4

A combination of phone number, work email address and social media credentials:
Brazil: **$1,931** China: **$145** Russia: **$200**

Source: http://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/

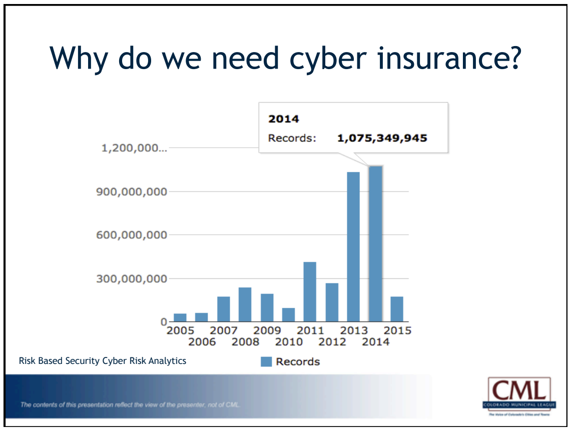
The contents of this presentation reflect the view of the presenter, not of CML.



Why do we need cyber insurance?

Risk Based Security Cyber Risk Analytics

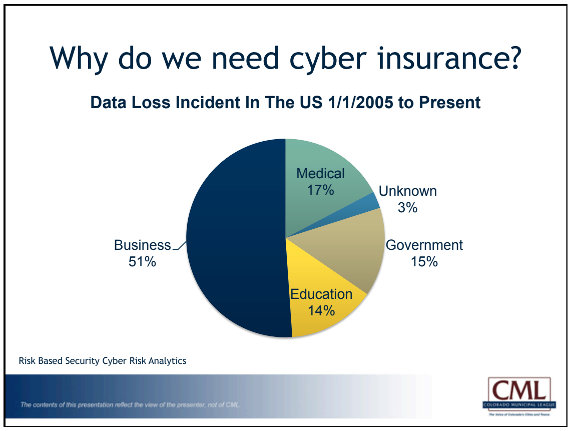
The contents of this presentation reflect the view of the presenter, not of CML.



Why do we need cyber insurance?

Risk Based Security Cyber Risk Analytics

The contents of this presentation reflect the view of the presenter, not of CML.

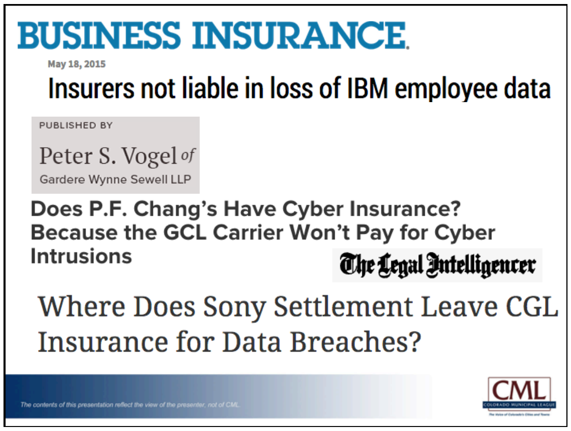


Why do we need cyber insurance?

Data Loss Incident In The US 1/1/2005 to Present

Risk Based Security Cyber Risk Analytics

The contents of this presentation reflect the view of the presenter, not of CML.



BUSINESS INSURANCE

May 18, 2015

Insurers not liable in loss of IBM employee data

PUBLISHED BY

Peter S. Vogel *of*

Gardere Wynne Sewell LLP

Does P.F. Chang's Have Cyber Insurance? Because the GCL Carrier Won't Pay for Cyber Intrusions

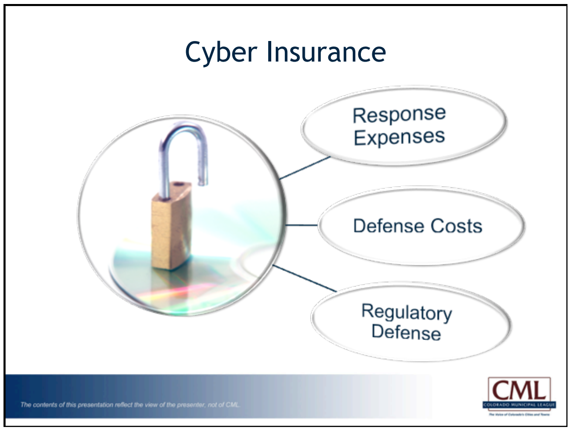
The Legal Intelligencer

Where Does Sony Settlement Leave CGL Insurance for Data Breaches?

The contents of this presentation reflect the view of the presenter, not of CML.

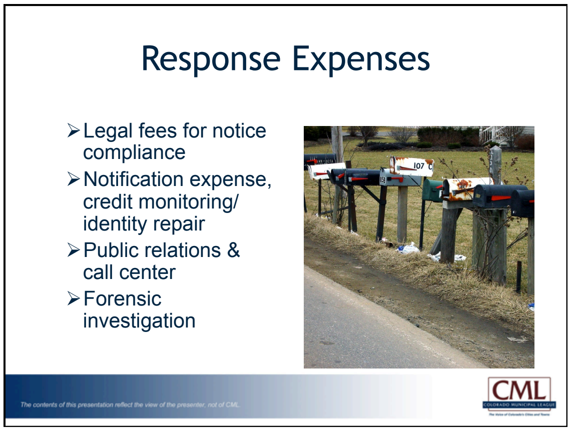
Cyber Insurance

The contents of this presentation reflect the view of the presenter, not of CML.



Cyber Insurance

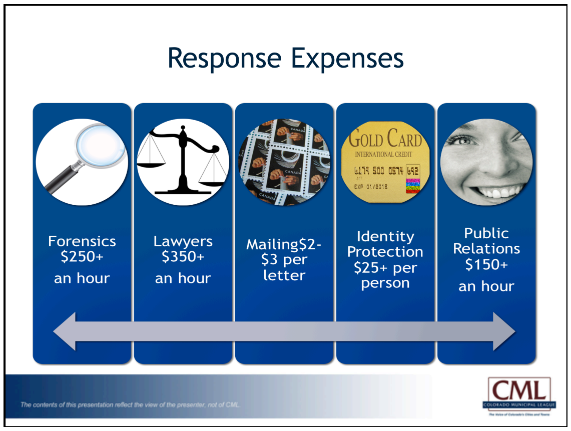
The contents of this presentation reflect the view of the presenter, not of CML.



Response Expenses

- ➢ Legal fees for notice compliance
- ➢ Notification expense, credit monitoring/ identity repair
- ➢ Public relations & call center
- ➢ Forensic investigation

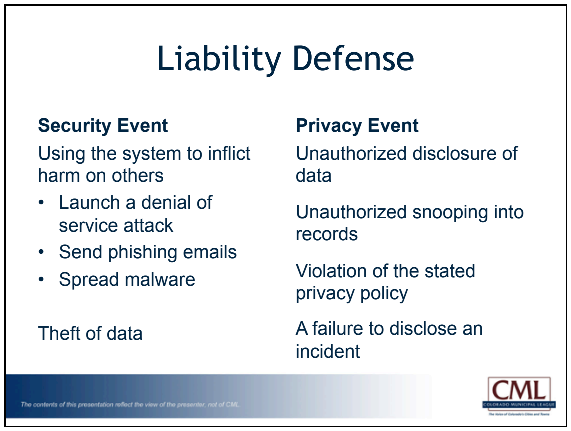
The contents of this presentation reflect the view of the presenter, not of CML.



Response Expenses

Forensics $250+ an hour	Lawyers $350+ an hour	Mailing$2-$3 per letter	Identity Protection $25+ per person	Public Relations $150+ an hour

The contents of this presentation reflect the view of the presenter, not of CML.



Liability Defense

Security Event

Using the system to inflict harm on others

- Launch a denial of service attack
- Send phishing emails
- Spread malware

Theft of data

Privacy Event

Unauthorized disclosure of data

Unauthorized snooping into records

Violation of the stated privacy policy

A failure to disclose an incident

The contents of this presentation reflect the view of the presenter, not of CML.

Regulatory Defense

Responding to investigations brought by privacy regulators

(regardless of whether private right of action)

because of a breach OR mishandling of personal information

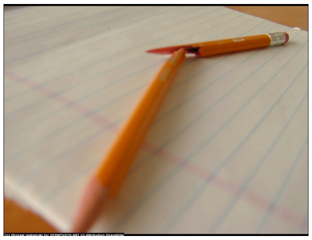
Regulatory Defense

Federal	State	Private
• FTC • GLBA • HIPAA • DPPA • COPPA • FERPA	• Notification • Attorneys General • Consumer Protection Agencies	• PCI-DSS

Cyber Insurance

As helpful as some of these policies can be, expect some things not to be covered

Reputation Damage

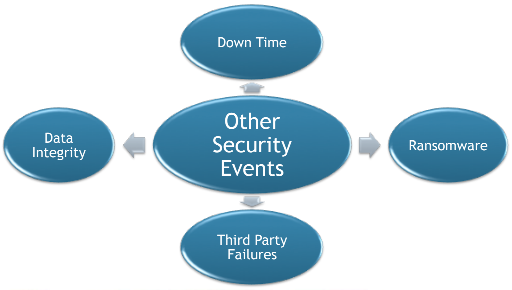


(C) Michael Jastremski for OPENPHOTO.NET CC-Attribution-ShareAlike

Michael Jastremski

Regular maintenance Upgrades Fixes

A Word About Words



Other Security Events

Down Time

Data Integrity

Ransomware

Third Party Failures

Key Take Aways

- ✓ Cyber coverage is an excellent tool for managing the cost of a data breach
- ✓ Responds to 1st party response costs, 3rd party damages and regulatory investigations
- ✓ Not a substitute for good data security practices
- ✓ There is more to security than data confidentiality – those events might not be covered

The contents of this presentation reflect the view of the presenter, not of CML.

Questions & Discussion

The contents of this presentation reflect the view of the presenter, not of CML.

Contact Information

Inga Goddijn
Executive Vice President
Managing Director of Insurance Services
Risk Based Security
(855) 727-7475 x703
Inga@riskbasedsecurity.com

Paul Nelson
Chief Architect
AppliedTrust
(303) 245-4532
paul@appliedtrust.com

Jeffrey A. Wells
City Manager
City of Fort Morgan
(970) 542-3973
jwells@cityoffortmorgan.com

Ken C. Price
CML Information Technology Section Chair
Information Services Director
City of Littleton
(303) 795-3722
kprice@littletongov.org

The contents of this presentation reflect the view of the presenter, not of CML.

Sources

GovInfoSecurity.com, Govtech.com, darkreading.com
Great sources of news, whitepapers and information about security

National Conference of State Legislatures
Website (www.ncsl.org) maintains a list of the state security breach notification & data disposal laws with links to the statutes.

SANS Critical 20
Website (www.sans.org) for information on the top 20 security controls every organization should implement.

Pcisecuritystandards.org
For all things PCI related, including self assessments, the full standards, links to qualified assessors and payment applications.

Privacyassociation.org
Great resource for information on privacy issues.

The contents of this presentation reflect the view of the presenter, not of CML.

Sources

Byres, E., & Lowe, J. (2004, October). The myths and facts behind cyber security risks for industrial control systems. *Proceedings of the VDE Kongress*, 116. Retrieved from http://www.controlglobal.com/assets/Media/MediaManager/The_Myths_and_Facts_behind_Cyber_Security_Risks.pdf

Finch, Carol. (2014, October 23). "Why do people hack?" Retrieved from www.ehow.com/about_4673738_why-do-people-hack.html

Grubbs, J. (2015, January 26). Officials: Fort Morgan on forefront of U.S. cybersecurity efforts. *Fort Morgan Times*. Retrieved from http://www.fortmorgantimes.com/News/ci_27396686/Officials:-Fort-Morgan-on-forefront-of-US-cybersecurity-efforts

Kaiser, Tiffany. (2013, February 21). Utility companies, government look to protect electric grid from hacks. *Daily Tech*. Retrieved from http://www.dailytech.com/Utility+Companies+Government+Look+to+Protect+Electric+Grid+from+Hacks/article29940.htm

Lowenberg, Tim Maj. Gen. (Ret.). "Emerging threats and vulnerabilities for the electricity sector: Ensuring Enterprise Resiliency." City of Fort Morgan Cyber Symposium. Country Steak Out, Fort Morgan, CO. 15 January 2015. Keynote Address.

Magnuson, Stew. (2014, March). "Power companies struggle to maintain defenses against cyber-attacks." National Defense Magazine. Retrieved from http://www.nationaldefensemagazine.org/archive/2014/March/Pages/PowerCompaniesStruggletoMaintainDefensesAgainstCyber-Attacks.aspx

Trend Micro. (2015, January 8). "Utilities under attack: New cyber security vector." Retrieved fromhttp://blog.trendmicro.com/utilities-attack-new-cyber-security-vector/

US Secret Service, National Threat Assessment Ctr, United States of America, CERT® Division of the Software Engineering Institute, United States of America, CSO Magazine, & United States of America. (2014). US cybercrime: Rising risks, reduced readiness key findings from the 2014 US state of cybercrime survey. Retrieved from https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=269621

Vinton, Kate. (2014, July 10) "Hacking gets physical: Utilities at rick for cyber attacks." Retrieved from http://www.forbes.com/sites/katevinton/2014/07/10/hacking-gets-physical-utilities-at-risk-for-cyber-attacks/

The contents of this presentation reflect the view of the presenter, not of CML.