CYBERSECURITY

RISK MANAGEMENT CASE STUDY

Scarlett Luis | ESE 527 Spring 2015 | April 26,2015

Schneider Electric TELVENT

AGENDA

- Case Introduction
  - Executive Summary
  - Major Actors & Stakeholders
  - Terminology
  - Vulnerabilities of Cyber war
- Historical Background
  - Timeline
  - Case Assessment
- Profile of the Enterprise
  - Roles of Stakeholders
  - Cybersecurity Risk Management Practices & Decisions
  - Failure Analysis
  - Stages of the Event
- Resilience Engineering History
- Lessons Learned/Questions for Discussions

CASE INTRODUCTION

EXECUTIVE SUMMARY

- On September 10, 2012, Telvent discovered a security breach to its corporate network.
- The attackers who breached the network installed malware and accessed project files related to Televent's smart grid product, OASyS SCADA DNA.
- According to security companies, such as Dell SecureWorks, McAfee, and Symantec, the digital fingerprints pointed to Comment Group, a Chinese hacking group.

MAJOR ACTORS & STAKEHOLDERS

TELVENT

Victim

Canadian IT & industrial automation company specializing in SCADA & IT systems for pipeline, energy utility, & environmental monitoring. It was acquired by Schneider Electric.

SCHNEIDER ELECTRIC

Victim

French company that specializes in electricity distribution, automation management, & produces installation components for energy management.

UTILITIES

REPSOL
ALSTOM
enagas
GDF SUEZ
TALISMAN
RED ELÉCTRICA
VATTENFALL
Madrileña
IBERDROLA
gasNatural
Fortum

Stakeholders

Clients worldwide that uses Telvent's SCADA system. Including: energy producing and distributing companies, rail transport companies, etc.

JOE STEWART

Actor

Director of malware research at SecureWorks. Expert on targeted attacks.

COMMENT GROUP/CREW

Alleged attacker

A Chinese hacking group that has stolen trade secrets and other confidential information from numerous foreign businesses and organizations .

TERMINOLOGY

Malware

- Short for malicious software
- Umbrella term to refer to intrusive software e.g. worms, spyware, ransomware
- Software is used to steal information or spy on computer users for an extended period without their knowledge
- It can take the form of executable code or scripts

Phishing

- The activity of defrauding an online account holder of financial information usually by posing as a legitimate company
- Hackers could create a clone of a website and tell you to enter personal information, which is then emailed to them
- Hackers commonly take advantage of these sites to attack people using them at their workplace or homes

TERMINOLOGY

Canadian Cyber Incident Response Center

- It assists in securing the vital cyber systems of provinces, territories, municipalities and private sector organizations while collaborating closely with partners

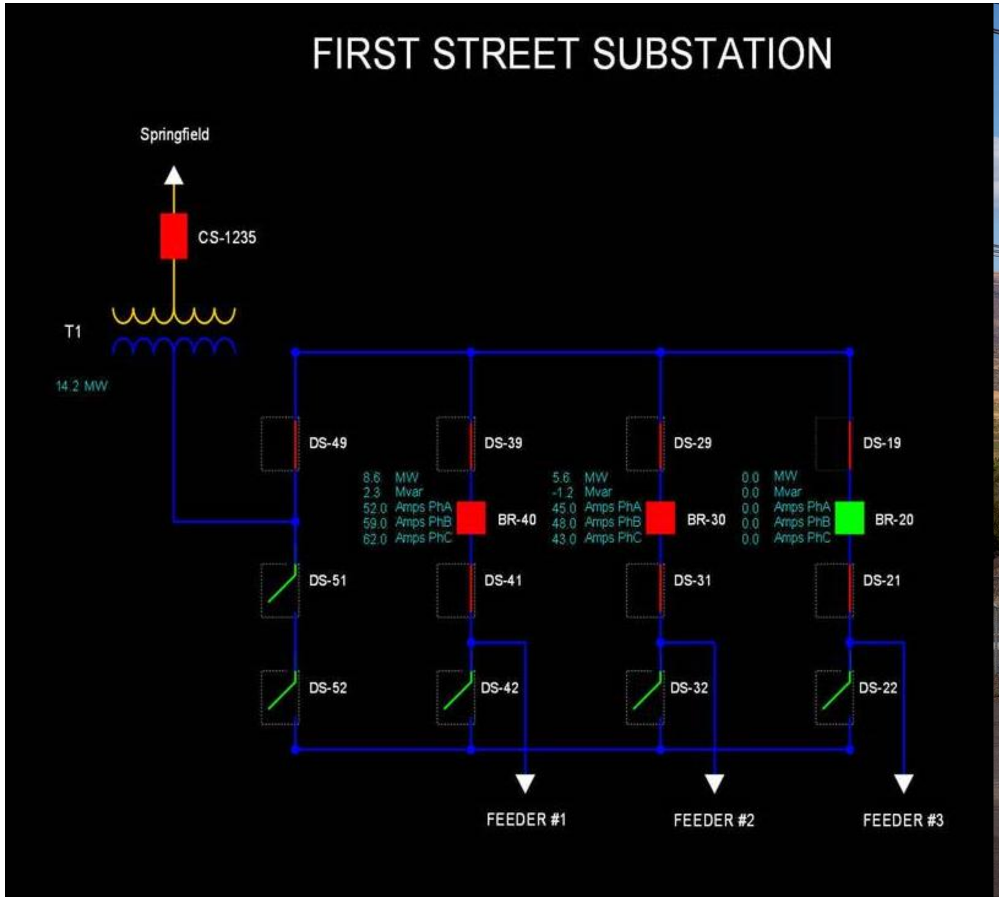
CCIRC

OASyS SCADA Dynamic Network of Applications (DNA)

- Real-time SCADA solution that bridges the typical gap between an enterprise network and activities in the field
- Delivers real-time data for critical business and operations decisions
- Was in deployment stage at the time of the attack

VULNERABILITIES OF CYBER WAR

Critical infrastructure controlled remotely are at risk of being damaged



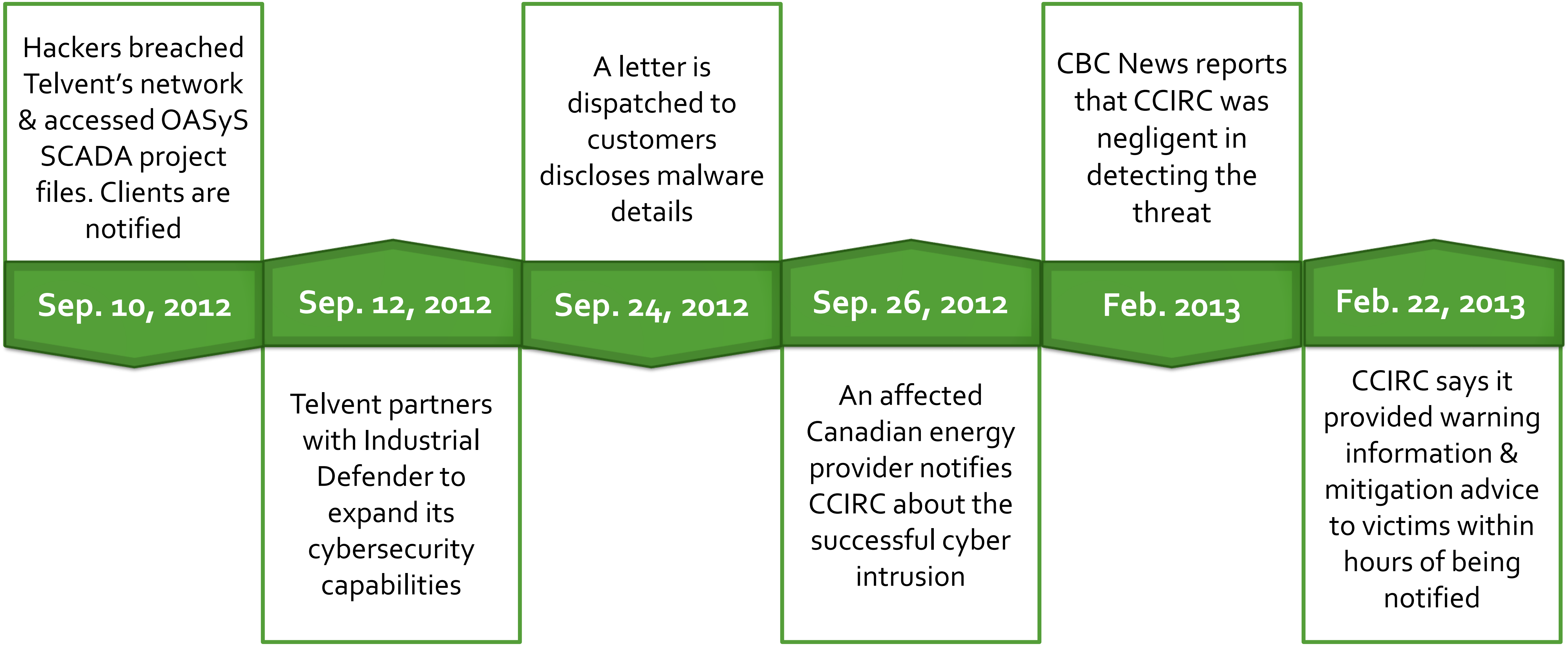
2 minutes of video

Example of SCADA system to monitor/control substations

Representation of a substation controlled remotely

HISTORICAL BACKGROUND

TIMELINE



Sep. 10, 2012

Hackers breached Telvent's network & accessed OASyS SCADA project files. Clients are notified

Sep. 12, 2012

Telvent partners with Industrial Defender to expand its cybersecurity capabilities

Sep. 24, 2012

A letter is dispatched to customers discloses malware details

Sep. 26, 2012

An affected Canadian energy provider notifies CCIRC about the successful cyber intrusion

Feb. 2013

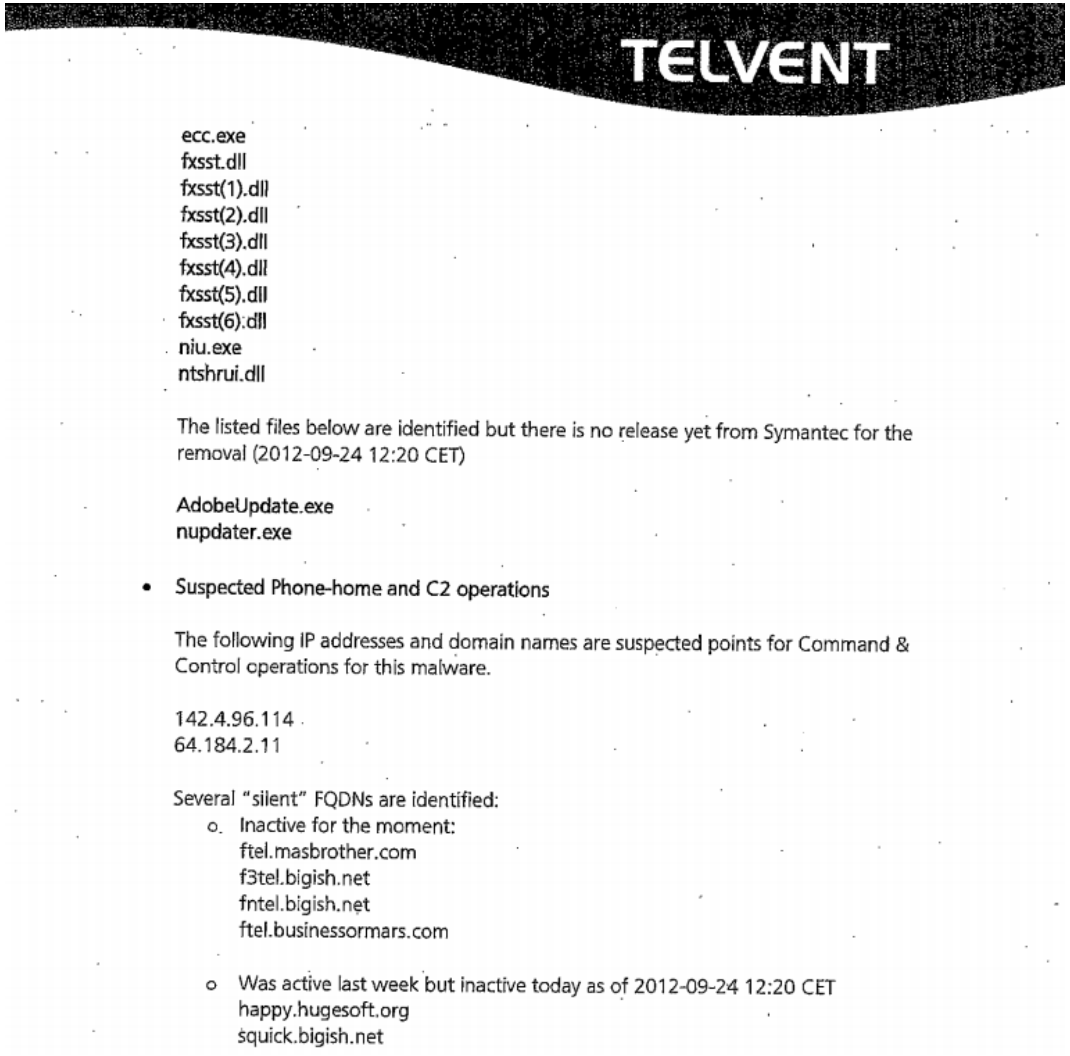
CBC News reports that CCIRC was negligent in detecting the threat

Feb. 22, 2013

CCIRC says it provided warning information & mitigation advice to victims within hours of being notified

Sep. 24, 2012

A page from an alert Telvent sent to customers about the malware left behind by the intruders



TELVENT

ecc.exe
fxsst.dll
fxsst(1).dll
fxsst(2).dll
fxsst(3).dll
fxsst(4).dll
fxsst(5).dll
fxsst(6).dll
niu.exe
ntshrui.dll

The listed files below are identified but there is no release yet from Symantec for the removal (2012-09-24 12:20 CET)

AdobeUpdate.exe
nupdater.exe

- Suspected Phone-home and C2 operations

The following IP addresses and domain names are suspected points for Command & Control operations for this malware.

142.4.96.114
64.184.2.11

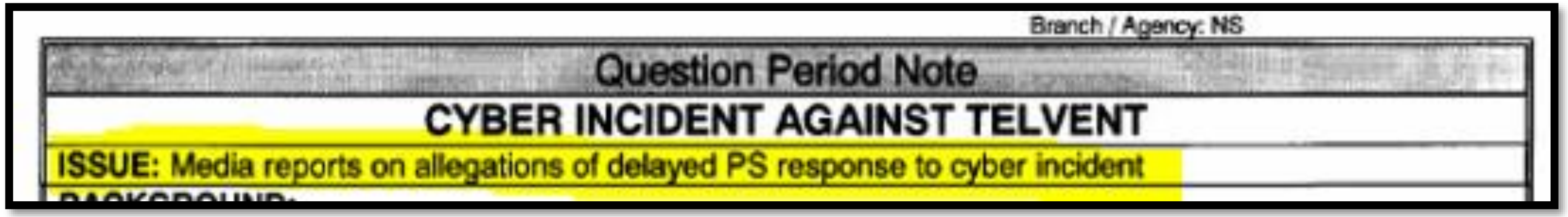
Several "silent" FQDNs are identified:

- Inactive for the moment:
  ftel.masbrother.com
  f3tel.bigish.net
  fntel.bigish.net
  ftel.businessormars.com

- Was active last week but inactive today as of 2012-09-24 12:20 CET
  happy.hugesoft.org
  squick.bigish.net

Late Feb. 2013

CBC News reported that CCIRC was negligent in detecting the threat



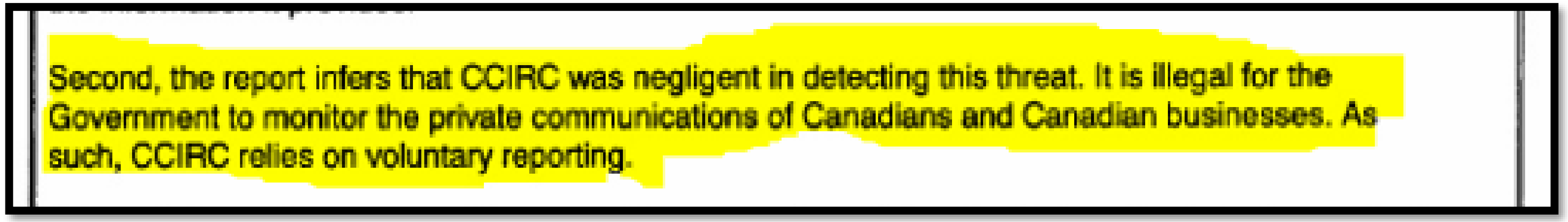
Branch / Agency: NS

Question Period Note

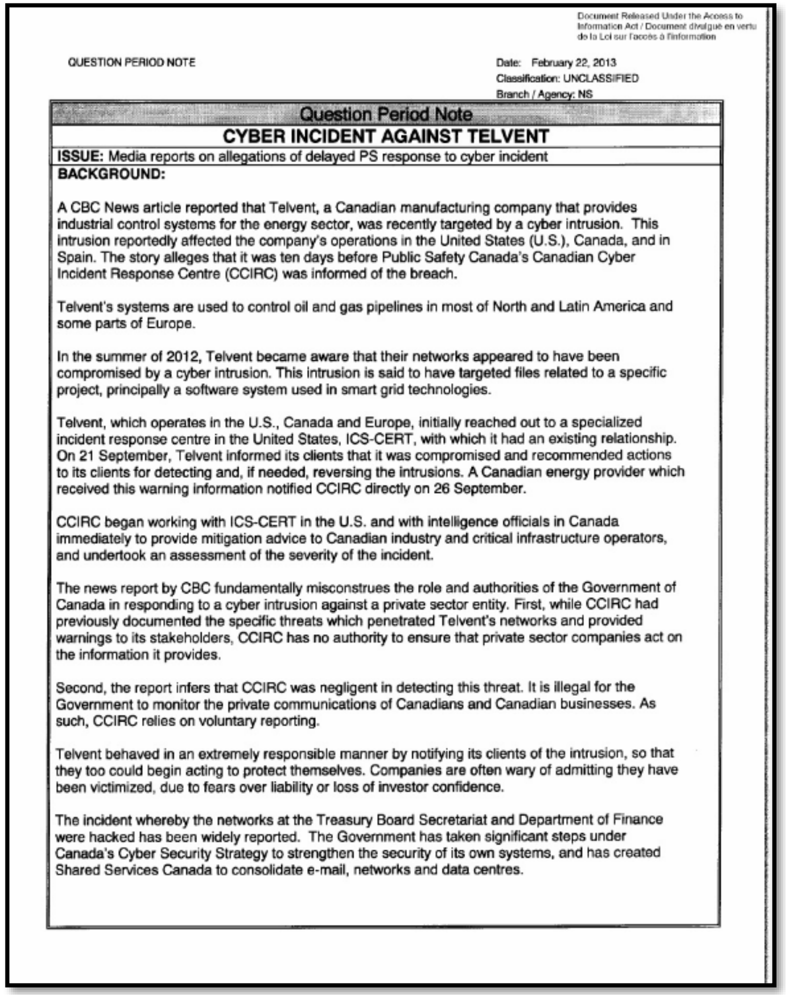
CYBER INCIDENT AGAINST TELVENT

ISSUE: Media reports on allegations of delayed PS response to cyber incident

During a briefing, CCIRC replies as shown in the excerpt below:



Second, the report infers that CCIRC was negligent in detecting this threat. It is illegal for the Government to monitor the private communications of Canadians and Canadian businesses. As such, CCIRC relies on voluntary reporting.



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

QUESTION PERIOD NOTE

Date: February 22, 2013
Classification: UNCLASSIFIED
Branch / Agency: NS

Question Period Note

CYBER INCIDENT AGAINST TELVENT

ISSUE: Media reports on allegations of delayed PS response to cyber incident

BACKGROUND:

A CBC News article reported that Telvent, a Canadian manufacturing company that provides industrial control systems for the energy sector, was recently targeted by a cyber intrusion. This intrusion reportedly affected the company's operations in the United States (U.S.), Canada, and in Spain. The story alleges that it was ten days before Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) was informed of the breach.

Telvent's systems are used to control oil and gas pipelines in most of North and Latin America and some parts of Europe.

In the summer of 2012, Telvent became aware that their networks appeared to have been compromised by a cyber intrusion. This intrusion is said to have targeted files related to a specific project, principally a software system used in smart grid technologies.

Telvent, which operates in the U.S., Canada and Europe, initially reached out to a specialized incident response centre in the United States, ICS-CERT, with which it had an existing relationship. On 21 September, Telvent informed its clients that it was compromised and recommended actions to its clients for detecting and, if needed, reversing the intrusions. A Canadian energy provider which received this warning information notified CCIRC directly on 26 September.

CCIRC began working with ICS-CERT in the U.S. and with intelligence officials in Canada immediately to provide mitigation advice to Canadian industry and critical infrastructure operators, and undertook an assessment of the severity of the incident.

The news report by CBC fundamentally misconstrues the role and authorities of the Government of Canada in responding to a cyber intrusion against a private sector entity. First, while CCIRC had previously documented the specific threats which penetrated Telvent's networks and provided warnings to its stakeholders, CCIRC has no authority to ensure that private sector companies act on the information it provides.

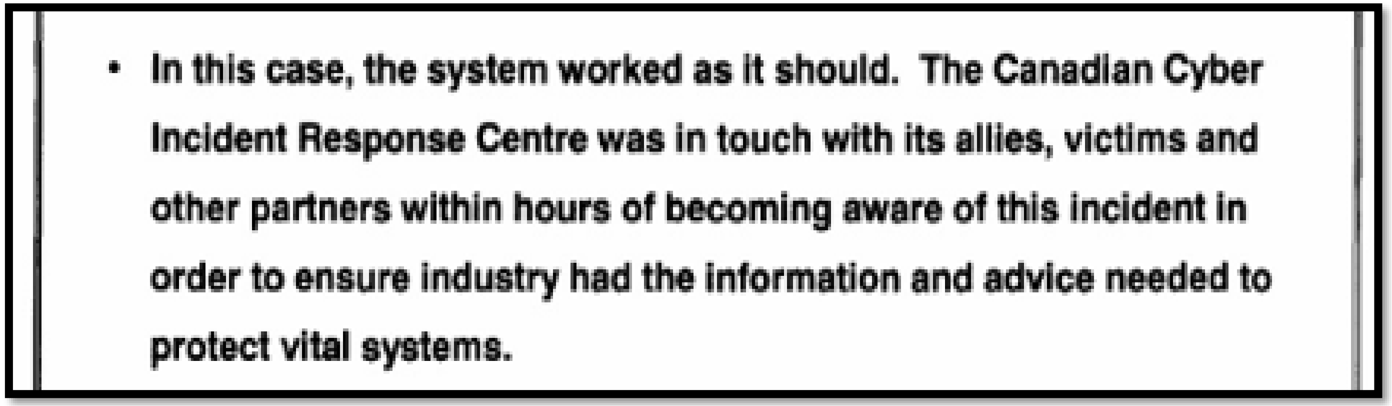
Second, the report infers that CCIRC was negligent in detecting this threat. It is illegal for the Government to monitor the private communications of Canadians and Canadian businesses. As such, CCIRC relies on voluntary reporting.

Telvent behaved in an extremely responsible manner by notifying its clients of the intrusion, so that they too could begin acting to protect themselves. Companies are often wary of admitting they have been victimized, due to fears over liability or loss of investor confidence.

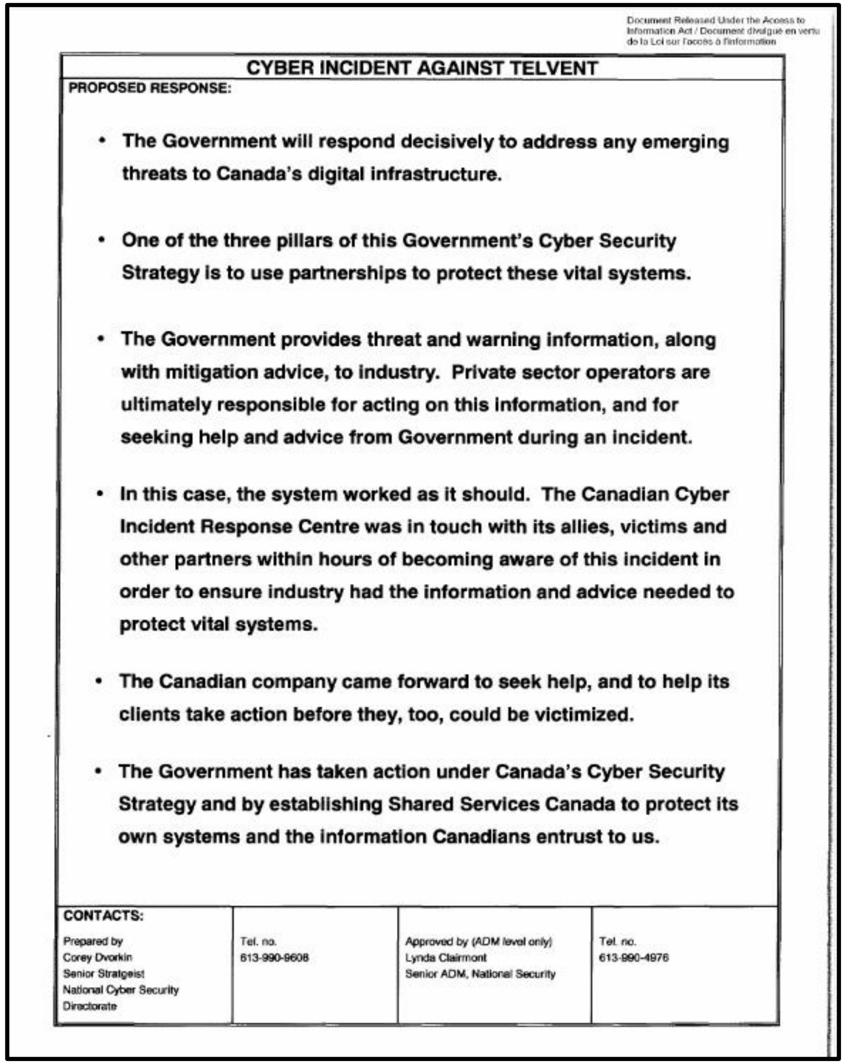
The incident whereby the networks at the Treasury Board Secretariat and Department of Finance were hacked has been widely reported. The Government has taken significant steps under Canada's Cyber Security Strategy to strengthen the security of its own systems, and has created Shared Services Canada to consolidate e-mail, networks and data centres.

Feb. 22, 2013

At the briefing, CCIRC says “it provided warning information & mitigation advice to victims in the industry within hours of being notified”



- In this case, the system worked as it should. The Canadian Cyber Incident Response Centre was in touch with its allies, victims and other partners within hours of becoming aware of this incident in order to ensure industry had the information and advice needed to protect vital systems.



Document Released Under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

CYBER INCIDENT AGAINST TELVENT

PROPOSED RESPONSE:

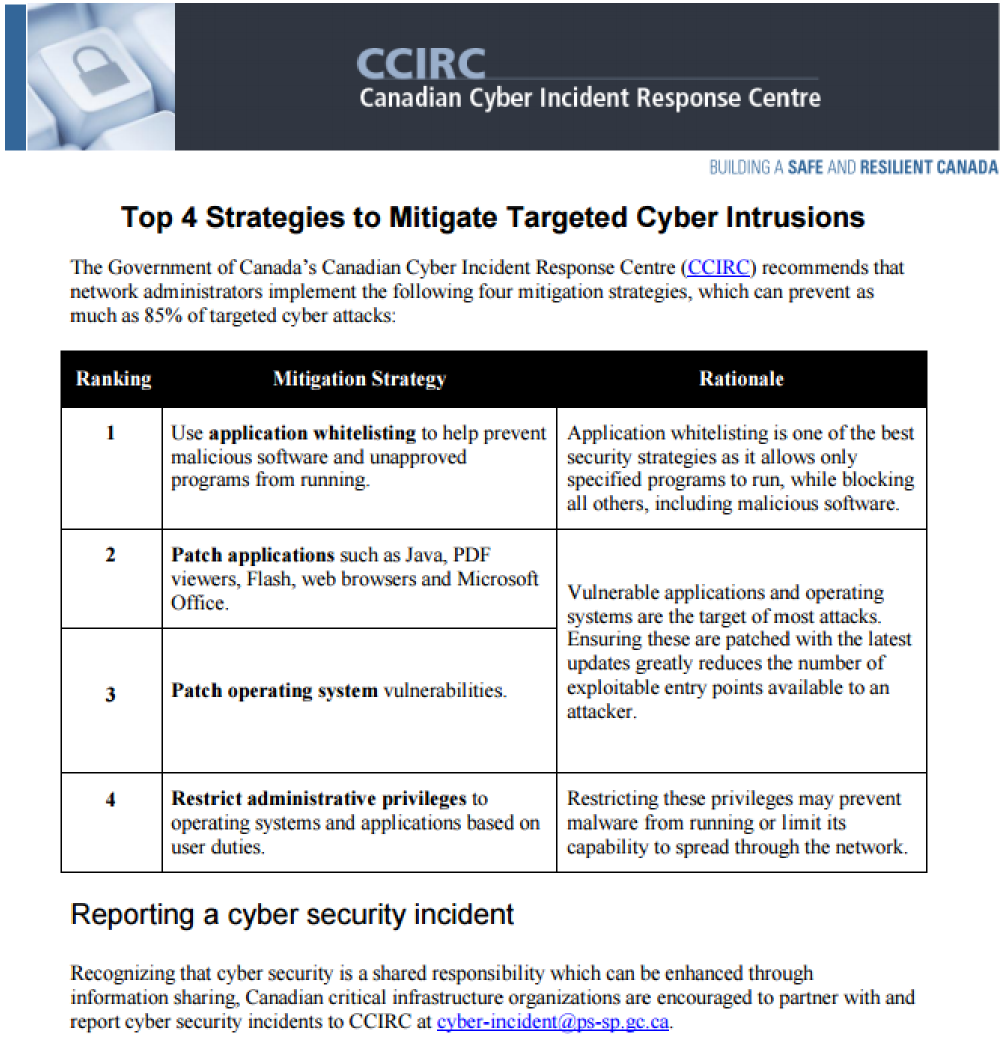
- **The Government will respond decisively to address any emerging threats to Canada's digital infrastructure.**
- **One of the three pillars of this Government's Cyber Security Strategy is to use partnerships to protect these vital systems.**
- **The Government provides threat and warning information, along with mitigation advice, to industry. Private sector operators are ultimately responsible for acting on this information, and for seeking help and advice from Government during an incident.**
- **In this case, the system worked as it should. The Canadian Cyber Incident Response Centre was in touch with its allies, victims and other partners within hours of becoming aware of this incident in order to ensure industry had the information and advice needed to protect vital systems.**
- **The Canadian company came forward to seek help, and to help its clients take action before they, too, could be victimized.**
- **The Government has taken action under Canada's Cyber Security Strategy and by establishing Shared Services Canada to protect its own systems and the information Canadians entrust to us.**

CONTACTS:			
Prepared by Corey Dvorkin Senior Stratgeist National Cyber Security Directorate	Tel. no. 613-990-9608	Approved by (ADM level only) Lynda Clairmont Senior ADM, National Security	Tel. no. 613-990-4976

Feb. 22, 2013

Excerpt from CCIRC's Website

Recommended mitigation strategies to avoid targeted cyber intrusions



CCIRC
Canadian Cyber Incident Response Centre

BUILDING A SAFE AND RESILIENT CANADA

Top 4 Strategies to Mitigate Targeted Cyber Intrusions

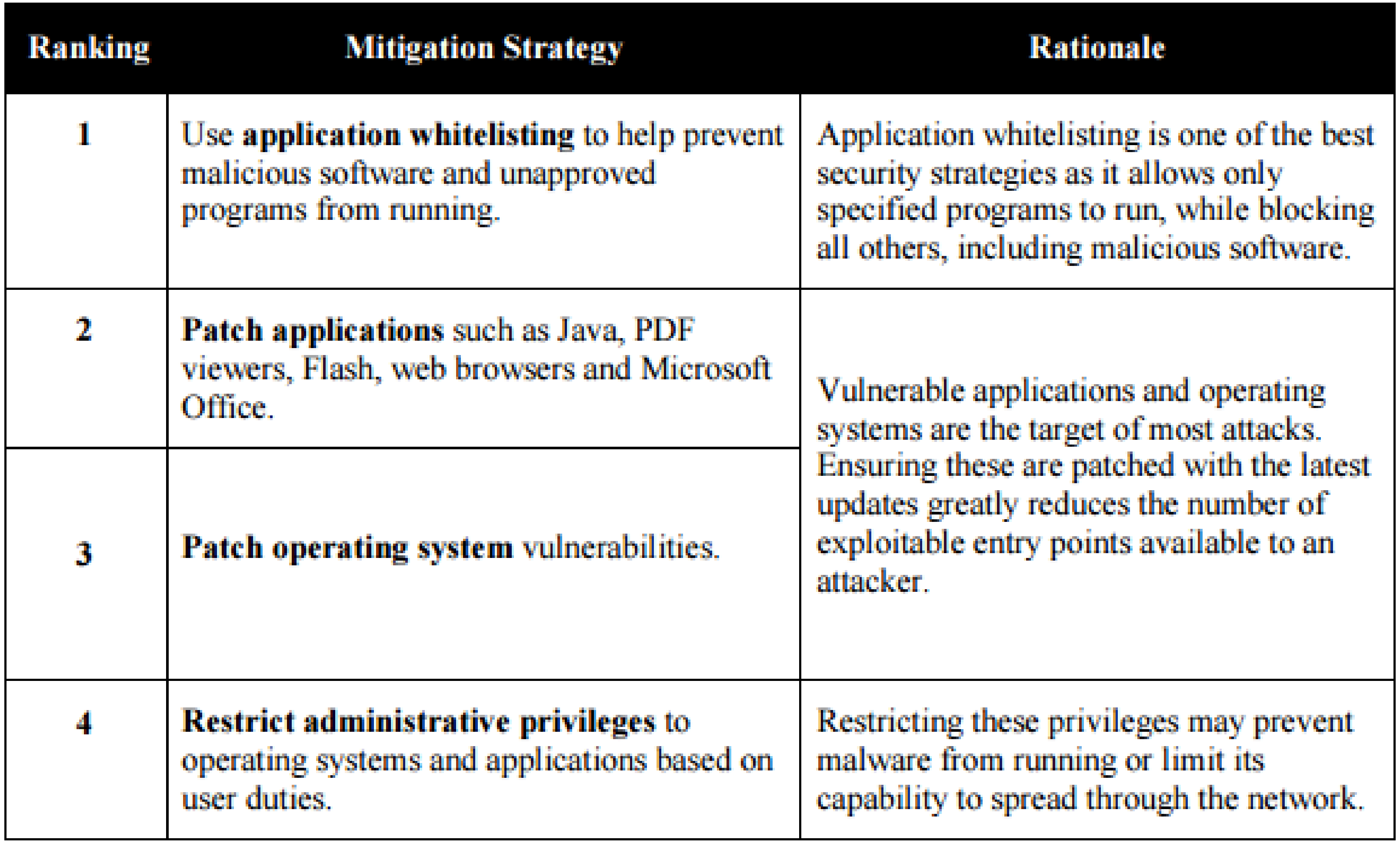
The Government of Canada's Canadian Cyber Incident Response Centre (CCIRC) recommends that network administrators implement the following four mitigation strategies, which can prevent as much as 85% of targeted cyber attacks:

Ranking	Mitigation Strategy	Rationale
1	Use **application whitelisting** to help prevent malicious software and unapproved programs from running.	Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
2	**Patch applications** such as Java, PDF viewers, Flash, web browsers and Microsoft Office.	Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
3	**Patch operating system** vulnerabilities.	
4	**Restrict administrative privileges** to operating systems and applications based on user duties.	Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

Reporting a cyber security incident

Recognizing that cyber security is a shared responsibility which can be enhanced through information sharing, Canadian critical infrastructure organizations are encouraged to partner with and report cyber security incidents to CCIRC at cyber-incident@ps-sp.gc.ca.

Feb. 22, 2013



Ranking	Mitigation Strategy	Rationale
1	Use **application whitelisting** to help prevent malicious software and unapproved programs from running.	Application whitelisting is one of the best security strategies as it allows only specified programs to run, while blocking all others, including malicious software.
2	**Patch applications** such as Java, PDF viewers, Flash, web browsers and Microsoft Office.	Vulnerable applications and operating systems are the target of most attacks. Ensuring these are patched with the latest updates greatly reduces the number of exploitable entry points available to an attacker.
3	**Patch operating system** vulnerabilities.	
4	**Restrict administrative privileges** to operating systems and applications based on user duties.	Restricting these privileges may prevent malware from running or limit its capability to spread through the network.

CASE ASSESSMENT

☑ **Successful Attack:**

Telvent’s internal firewall & security systems breached

? **Degree of Breach:**

- Scope of outcome not fully disclosed
- *“There was no evidence the attackers ever had the ability to access customers’ networks.”* -Schneider Electric
- *“The security breach of its corporate network affected some customer files.*" –Telvent Canda

☑ **Incident Mitigated:**

- Telvent disconnected the usual data links between clients and affected portions of its internal networks
- CCIRC worked with stakeholders in government & private sector to ensure they had the information & advice needed to protect vital systems

PROFILE OF THE ENTERPRISE

ROLES OF STAKEHOLDERS

- **Telvent**
  - Targeted vendor who addressed the situation immediately by alerting customers & adjusting their security processes
  - The firm would not reveal whether the hackers managed to steal information that might endanger any of the country's major utilities
- **Schneider**
  - Sought to preserve customer trust by ensuring that the situation was being handled accordingly
  - Did not want to divulge too much information
- **Customers/Users**
  - Were actively informed about the status of the attack
  - One client served as an informant to the emergency response team
  - Impact to customers of the energy providers in unknown
- **CCIRC (Cybersecurity Team/Emergency Response Team)**
  - Responded by mitigating the situation after being notified
- **U.S. Government/ Security Officials**
  - Discussions & fear of vulnerabilities in SCADA systems leading to serious damage of critical infrastructure renewed

CYBERSECURITY RISK MANAGEMENT PRACTICES & DECISIONS

Best Practices in Software Development

- Use Agile software development
- Coders work in pairs
- To introduce malware into an application in an Agile system would likely require the complicity of everyone on the sub-team

Best Practices in Software Testing

- Second level of security
- Machine-based testing simulate multi-user conditions and highly repetitive tasks
- Automated test scripts can discover functional anomalies which serve as base triggers for malware

Gaps and Ongoing Improvements

- Harmonization of methodology and security practices
- Securing implementations
- Ongoing surveillance of implemented technology
- Future deployments using cloud computing technology

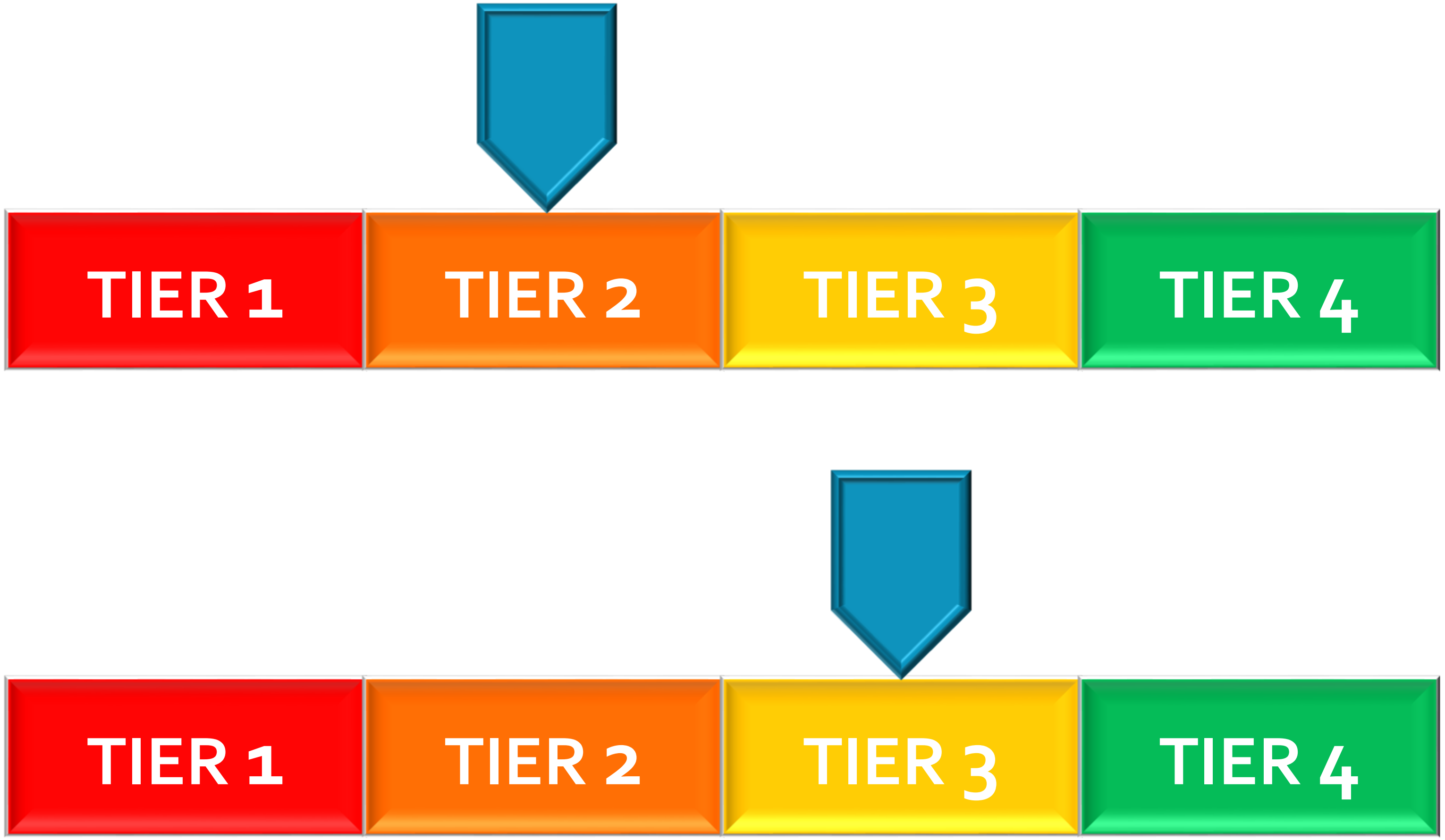
NIST MATURITY LEVELS

Target Profile	Description
Tier 1: Partial	Ad hoc risk management process; limited insight into risks; no collaboration with others
Tier 2: Risk Informed	Some processes and programs established, but not at the enterprise level; no formal external collaboration
Tier 3: Repeatable	Formal process and programs established at the enterprise level; some external collaboration
Tier 4: Adaptive	Ongoing, proactive and collaborative risk management process; deeply embedded in organizational culture

NIST MATURITY RATING

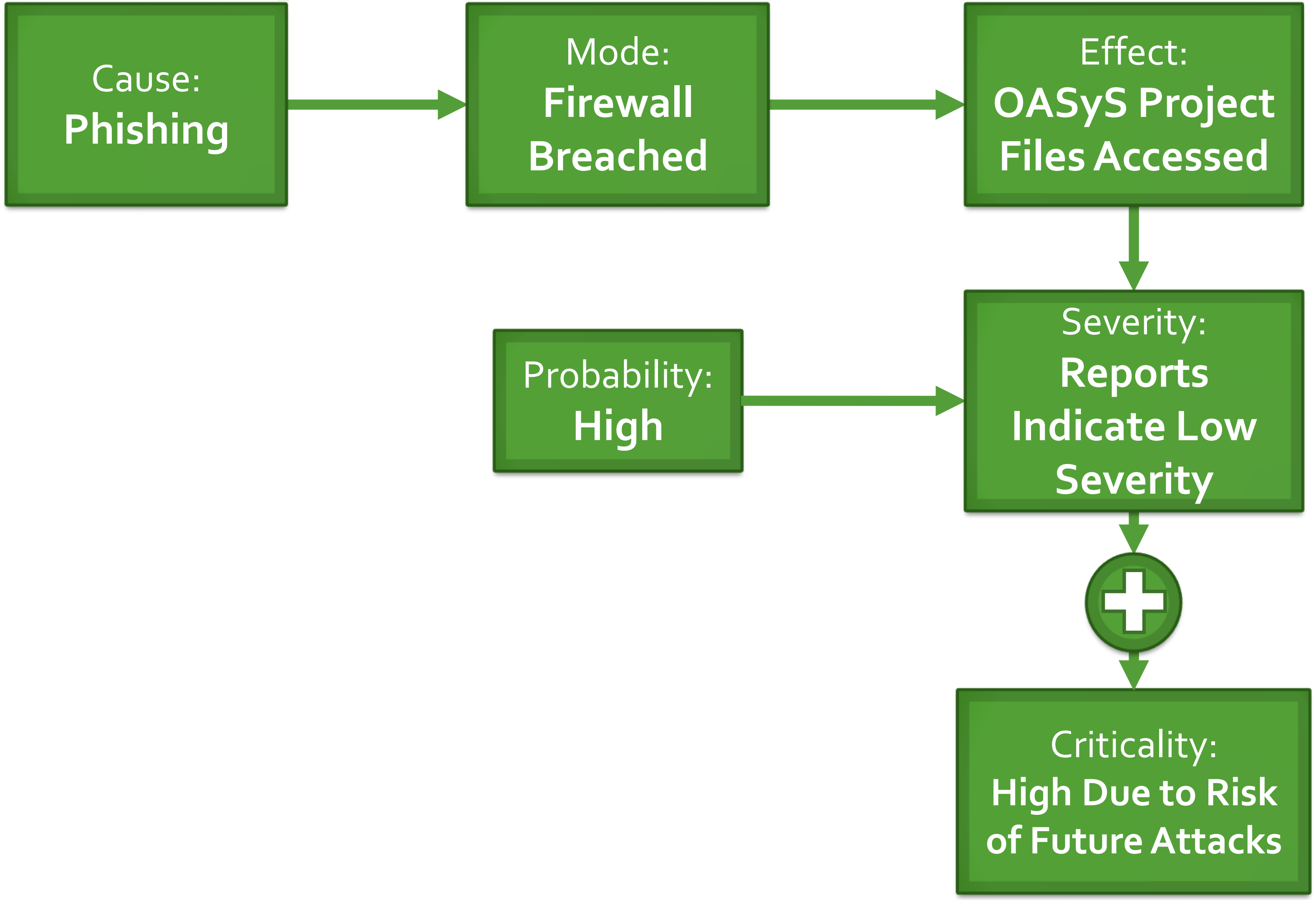
Before
Cyber Attack

After
Cyber Attack



FAILURE ANALYSIS

Failure Analysis



Cause: **Phishing**

Mode: **Firewall Breached**

Effect: **OASyS Project Files Accessed**

Probability: **High**

Severity: **Reports Indicate Low Severity**

Criticality: **High Due to Risk of Future Attacks**

STAGES OF THE EVENT

Pre-Event Good security reputation

- “Telvent has a good reputation in implementing security controls and responding to reported vulnerabilities”– Dale Peterson, Digital Bond

During Event Common security practices changed

- The usual method of connecting to customers was terminated to offset the attack
- In written communication to customers, the company detailed ongoing efforts to ascertain the scope and duration of the breach

Post-Event Comment Group investigated

- Investigation looked at data gathered by 30 security researchers, who tracked the Comment Group’s activity over less than two months last year & uncovered evidence that it had infiltrated at least 20 organizations
- Comment group attacks are associated with Comment Crew

RESILIANCE ENGINEERING

- What worked well?
  - Telvent's fast response & willingness to adopt changes
  - Immediate & continued communication with stakeholders
  - Mitigation strategies
  - Timing

- What didn't work well?
  - Human error

- The incident did & has fostered High Reliability Organization (HRO) characteristics/mindful principles

LESSONS LEARNED

- The best way to attack an environment with a firewall is to break it from the inside
- Humans are usually the weakest point in any system
  - Reason why phishing is so effective
- Computers are only as smart as the users who make them
  - Delivering a system in a secure fashion does not guarantee that it will remain so indefinitely

QUESTIONS FOR DISCUSSION

- Privacy vs. Security
  - What is the right balance?
- Should grade schools offer/require cybersecurity education?

THANK YOU

QUESTIONS?

REFERENCES

[1]O. Jordan Press, O. Read more Articles from Jordan Press and O. Jordan Press, "Telvent client alerted feds to hack at energy company, documents suggest", *canada.com*, 2013. [Online]. Available: http://o.canada.com/news/national/telvent-client-alerted-feds-to-hack-at-energy-company-documents-suggest. [Accessed: 14- Apr- 2016].

[2]K. Zetter, "Maker of Smart-Grid Control Software Hacked", *WIRED*, 2016. [Online]. Available: http://www.wired.com/2012/09/scada-vendor-telvent-hacked/. [Accessed: 14- Apr- 2016].

[3]"TGS-BP-BusinessPresentation-en-roo", *Slideshare.net*, 2016. [Online]. Available: http://www.slideshare.net/Simplify-IT-Complexity/tgs-bpbusiness-presentationenroo/20. [Accessed: 26- Apr- 2016].

[3]"Top 4 Strategies to Mitigate Targeted Cyber Intrusions", *Publicsafety.gc.ca*, 2015. [Online]. Available: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-eng.aspx. [Accessed: 26- Apr- 2016].http://usresilienceproject.org/wp-content/uploads/2014/09/pdf-USRP_Telvent_CS_030812.pdf

[4]"Top 4 Strategies to Mitigate Targeted Cyber Intrusions", *Publicsafety.gc.ca*, 2015. [Online]. Available: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/tp-strtgs-eng.aspx. [Accessed: 26- Apr- 2016].

[5]"Hackers infiltrate Calgary-based technology firm", *Cbc.ca*, 2016. [Online]. Available: http://www.cbc.ca/news/canada/hackers-infiltrate-calgary-based-technology-firm-1.1231641. [Accessed: 26- Apr- 2016].

[6]"Telvent Hit by Sophisticated Cyber-Attack, SCADA Admin Tool Compromised | SecurityWeek.Com", *Securityweek.com*, 2016. [Online]. Available: http://www.securityweek.com/telvent-hit-sophisticated-cyber-attack-scada-admin-tool-compromised. [Accessed: 26- Apr- 2016].https://threatpost.com/attack-scada-vendor-telvent-raises-concerns-092712/77056/

[7]L. Vaas and L. Vaas, "Chinese hackers linked to breach of control systems used in electric grids", *Naked Security*, 2012. [Online]. Available: https://nakedsecurity.sophos.com/2012/09/27/chinese-hackers-linked-to-breach-of-control-systems-used-in-electric-grids/. [Accessed: 26- Apr- 2016].http://www.wired.com/2012/09/scada-vendor-telvent-hacked/

[8]"Chinese Hackers Blamed for Breach of Telvent's SCADA-Related Network", *POWER Magazine*, 2012. [Online]. Available: http://www.powermag.com/chinese-hackers-blamed-for-breach-of-telvents-scada-related-network/. [Accessed: 26- Apr- 2016].

[9]C. Oliver Joy, "Mandiant: China is sponsoring cyber-espionage - CNN.com", *CNN*, 2016. [Online]. Available: http://www.cnn.com/2013/02/19/business/china-cyber-attack-mandiant/. [Accessed: 26- Apr- 2016].

[10]"Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent", 2012.