OSIsoft®

USERS CONFERENCE 2016

April 4-8, 2016 | San Francisco

TRANSFORM YOUR WORLD

Cyber Security for Industrial IT

Exploring Partnership for Effective Incident Response

Presented by

Bryan Owen, OSIsoft – Principal Cyber Security Manager

Ryan Cheff, Chevron – Manufacturing Technical Architect

Agenda

- Why Incident Response?
  - Case Study: Stolen Credentials
- OSIsoft Policy
  - Ethical Disclosure
- Chevron Approach
  - Vendor Escalation & Coordination

Who's next?

Hollywood hospital hit with ransomware:

Hackers demand $3.6 million ransom

Credit: Shutterstock

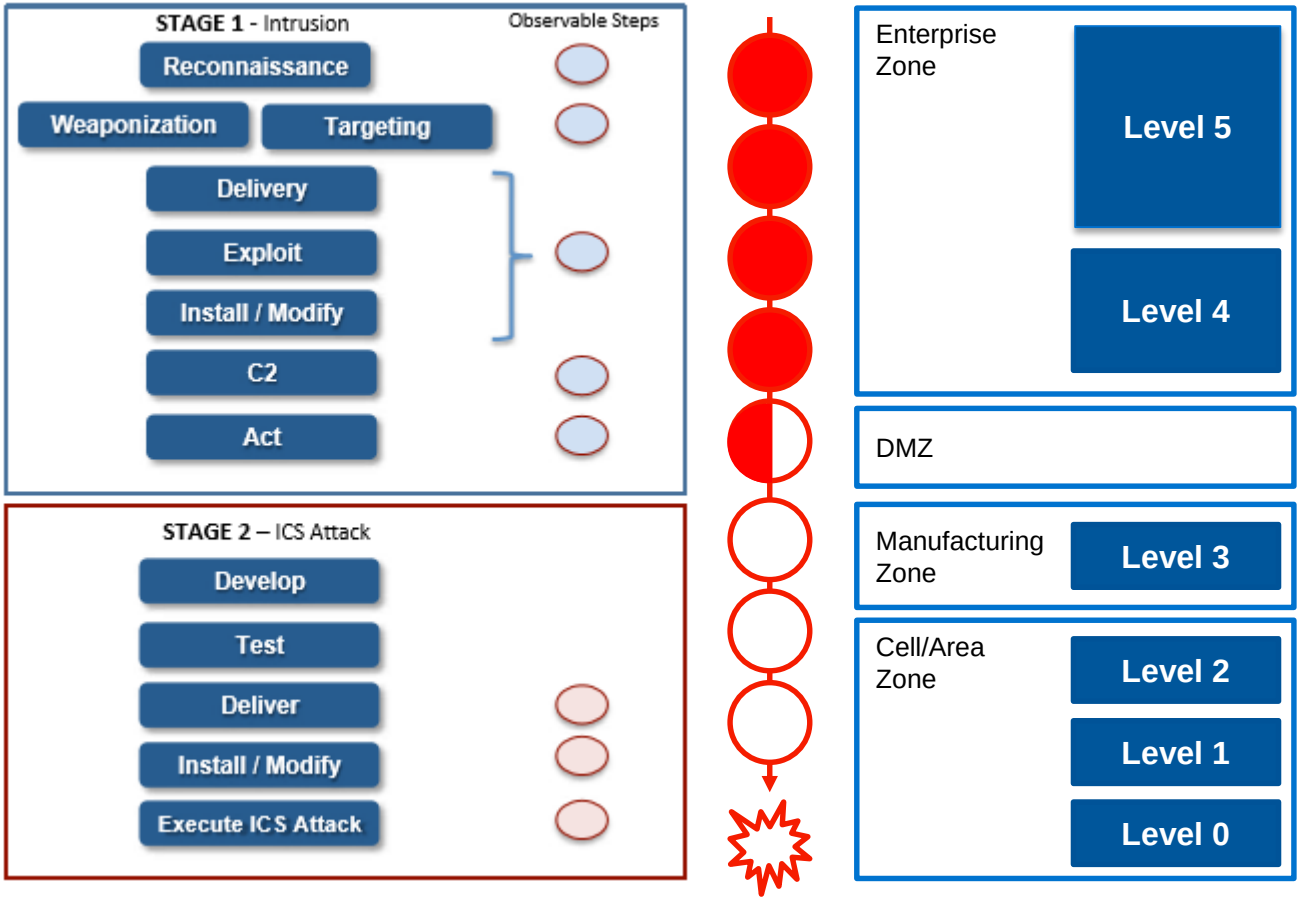
Ransomware has locked up a Hollywood hospital's computers for over a week as hackers demand $3.6 million in ransom.

Computerworld | Feb 15, 2016 6:39 AM PT

NIST CSF Core Functions – “Respond/Recover”

…plans to take action regarding a detected cybersecurity event…

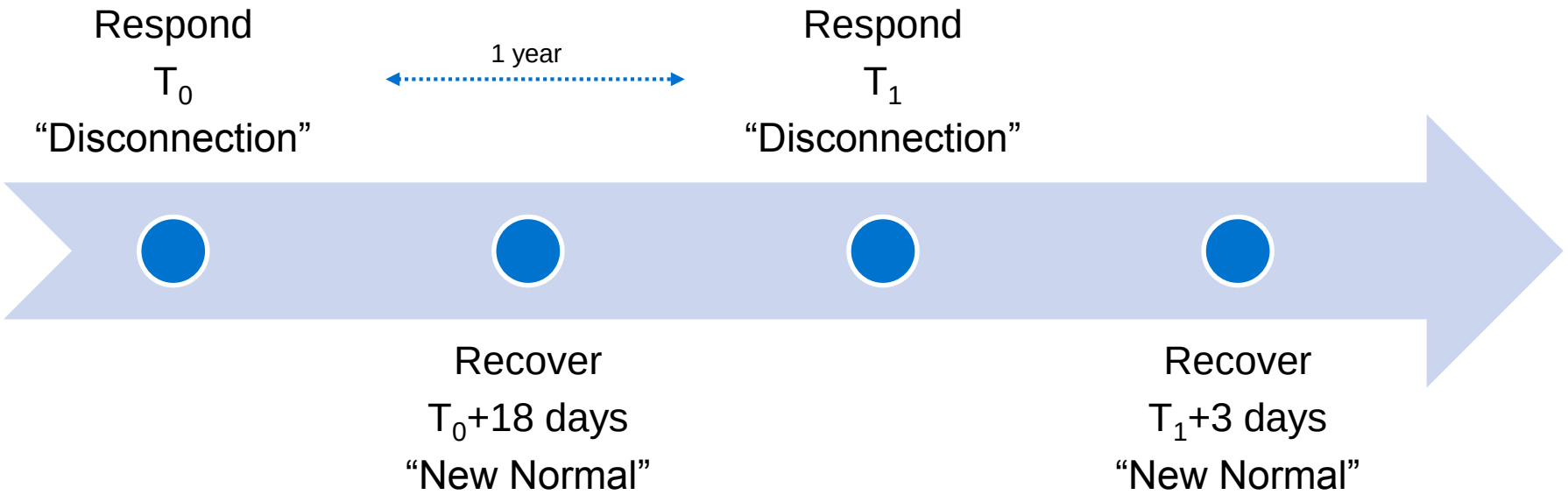
…plans for resilience and to restore any capabilities or services that were impaired…



Attack with Impact

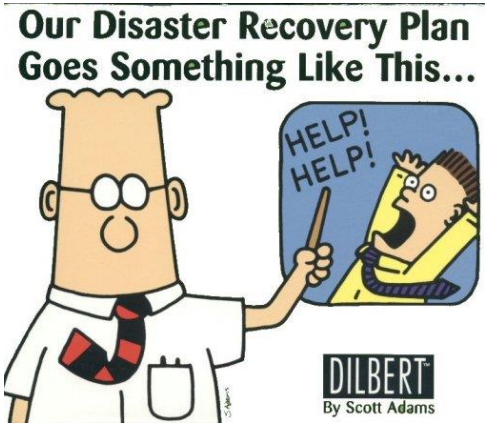
Case Study

Timeline



Respond/Restore – Urgent Questions

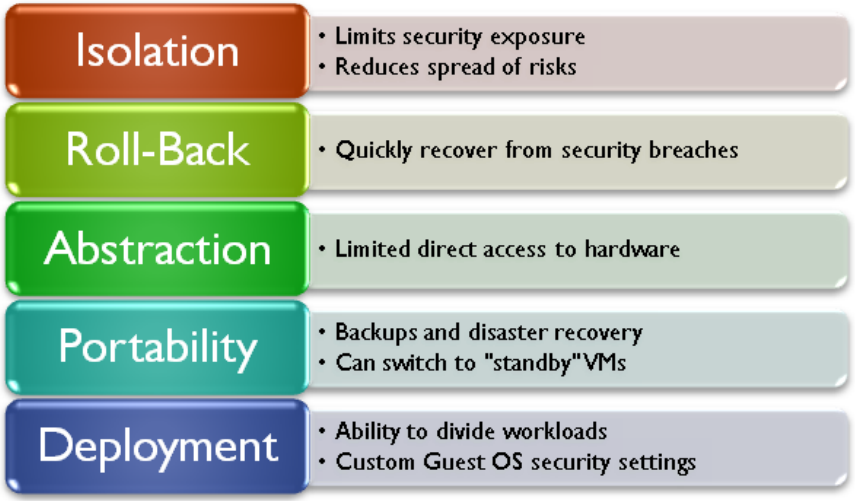
- Could attacker use stolen credentials to actuate control?
- How to disconnect without losing data?
- How are passwords stored?
- How to restore the PI System?
- Security by obscurity?
  - changing host name,
  - IP address,
  - TCP port

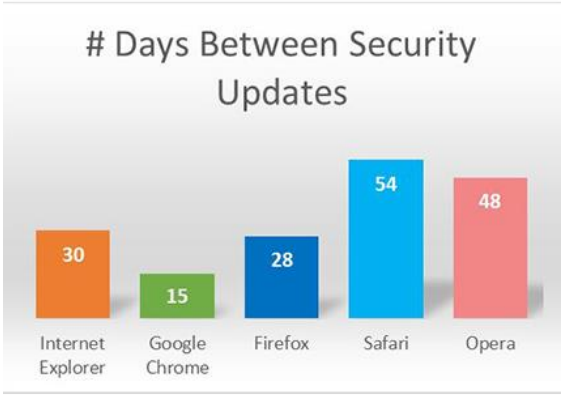


Respond/Recover – Lessons Learned

- Have a plan, 2nd time was ‘rote execution’
- Contain control protocol and credential use by zone
- Shift majority of user load to application servers
- Implement virtualization
- Allow remote access

(OSIsoft Technical Support)





What about Vulnerabilites?

Ethical Disclosure

- Disclose vulnerabilities in a predictable and reliable process
- Provide actionable information
- Empower our customers, not would-be attackers

https://techsupport.osisoft.com/Troubleshooting/Ethical-Disclosure-Policy

Vulnerability Disclosure Process

OSIsoft Discovered Vulnerabilities

- Generate remediation plan and security bulletins for high and medium level issues
- Communicate actionable information: release of a product update, avoidance procedure, …
- Release security bulletins on the 2nd Tuesday of the month
- Communicate with customers and partners one month prior to any public service (example: ICS-CERT)

3rd Party Discovered Vulnerabilities

- Work with the 3rd party to replicate the **OSIsoft Discovered Vulnerability** process
- Adjust as necessary to keep the 3rd party engaged as a partner in the resolution
- Engage the 3rd party in testing the actionable information before release
- Recognize the 3rd party's work, give them the recognition they deserve

Actively-exploited Vulnerabilities

- Actively engage partners and customers with recommended defenses and guidance on vulnerabilities being exploited
- Engage with customers immediately, do not wait to follow the regular cycle of patch or software release
- Provide software updates addressing vulnerabilities as soon as available
- Involves senior leadership within the company to ensure adequacy of resources and timeliness of response

Customer Perspective: Chevron Approach

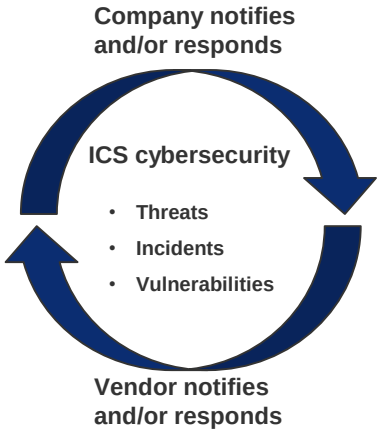
Building relationships with key automation vendors

Chevron's approach to automation vendor escalation and coordination

Objective

Establish enterprise-level relationships with key automation vendors to:

- build proactive security posture
- facilitate an effective response when attacks target the ICS infrastructure
- establish quality standards for security support



Scope

- Process control, safety system, SCADA, power and electrical systems vendors
- Integrate vendor & company security Roles & Responsibilities
- Publish standards guidance for contract cyber language
- Implement on-going relationship charter

Value to Chevron

- Knowledge of who to call at the vendor, when and why
- Common understanding of expected response from vendors
- Reduce duplication of work for both facility owners and vendors to individually determine and manage security services
- Enterprise incident response plan

"Ideal state"

Cyber incident response and escalation "customer quick reference guide"
Disclosure of important security vulnerabilities ahead of "the fix"
Issue security advisories in embedded 3rd party software products (operating systems, databases, network gear)
Security configuration, hardening, maintenance guides and audit tools
Software security patches and updates for life of the product. Access to critical fixes regardless of a support contract
Access to "end-of-support" timelines to assist with mitigation planning
Vendor independent security testing throughout products' support life
Enterprise-level cybersecurity service management role
Tabletop walk-throughs to validate the mutual understanding of as-is process

Incident Response – Call to Action

Next Week

- Ask: “Is our cyber incident planning is on par with companies who have had a serious breach?”

3 Months

- Work with business to set incident response goals for important OT functions.

Year End

- Understand current response capability including key suppliers of OT systems.

Questions

Please wait for the **microphone** before asking your questions

State your **name & company**

Please remember to…

Complete the Online Survey for this session

http://ddut.ch/osisoft

감사합니다

谢谢

Danke

Merci

Gracias

Thank You

ありがとう

Спасибо

Obrigado

The last frontier for untapped profits ….

…. **Asset Performance Management**

Suggested Conference Presentations

Day	Time	Agenda
Tue	10AM	Understanding and Mitigating Risk (PGE)
Tue	4:30PM	Bow-Tying It All Together (Monsanto)
Wed	9:45AM	Mission Critical Infrastructure (Qualcomm)
Wed	2:45PM	Exploring Partnership for Effective Incident Response
Wed	3:30PM	Using the PI System to Create a Smart Campus (UC Davis)
Thu	9:30AM	PI Server 2016: The Modern PI System
Thu	1:20PM	Roadmap for PI Connectors and PI Interfaces

Security Partners in the Expo Booth

FOX IT
FOR A MORE SECURE SOCIETY

Luminant

Owl Computing Technologies, Inc.

WATERFALL®
One Way to Connect

Cybersecurity PI User Groups

Join to discuss best practices, white papers, share news, and exchange ideas.

Objectives:

- Identify Best Practices
- Share knowledge and ideas across our users
- Foster communication with OSIsoft regarding industry needs

This is NOT an avenue for sales presentations or marketing

Want to opt in?
https://pisquare.osisoft.com/groups/security

Or contact jsirois@osisoft.com

Have questions?

- jsirois@osisoft.com
- brian@osisoft.com
- bryan@osisoft.com
- Visit the PI Square and Security Booths


OSIsoft.
USERS CONFERENCE 2016
April 4-8, 2016 | San Francisco
TRANSFORM
YOUR WORLD