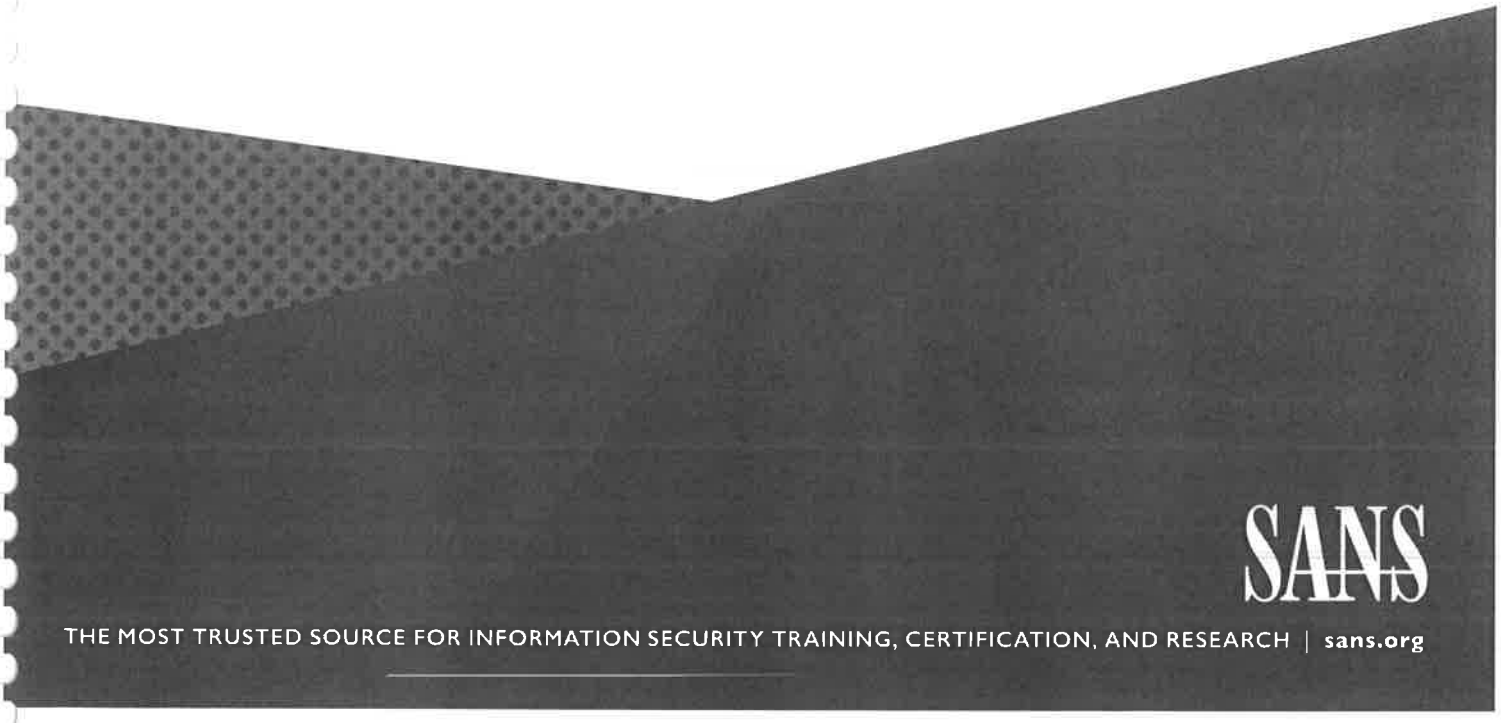
410.5
ICS Security Governance



SANS

ICS410.5 | ICS/SCADA Security Essentials

SANS

ICS Security Governance

The **SANS ICS 410**, ICS/SCADA Security Essentials course, was developed by a collection of experts whose diverse work experiences, knowledge, and skills truly blend together to cover the very specific content areas for this course.

Justin Searle is the Director of ICS Security at InGuardians, specializing in ICS security architecture design and penetration testing. Justin led the Smart Grid Security Architecture group in the creation of NIST Interagency Report 7628 and has played key roles in the Advanced Security Acceleration Project for the Smart Grid (ASAP-SG), National Electric Sector Cybersecurity Organization Resources (NESCOR), and Smart Grid Interoperability Panel (SGIP). Justin has taught courses in hacking techniques, forensics, networking, and intrusion detection for multiple universities, corporations, and security conferences. He is currently a Senior Instructor for the SANS Institute. In addition to electric power industry conferences, Justin frequently presents at top international security conferences such as Black Hat, DEFCON, OWASP, Nullcon, and AusCERT. Justin co-leads prominent open source projects including the The Control Thing Platform, Samurai Web Testing Framework (SamuraiWTF), Samurai Security Testing Framework for Utilities (SamuraiSTFU), Yokoso!, and Laudanum. Justin has an MBA in International Technology and is a CISSP and SANS GIAC certified Incident Handler (GCIH), Intrusion Analyst (GCIA), Web Application Penetration Tester (GWAPT), and GIAC Industrial Control Security Professional (GICSP).

Dr. Eric Cole is an industry-recognized security expert with over 20 years of hands-on experience. Dr. Cole has experience in information technology with a focus on helping customers focus on the right areas of security by building out a dynamic defense. Dr. Cole has a master's degree in computer science from NYIT and a doctorate from Pace University with a concentration in information security. He served as CTO of McAfee and Chief Scientist for Lockheed Martin. Dr. Cole is the author of several books, including *Advanced Persistent Threat*, *Hackers Beware*, *Hiding in Plain Sight*, *Network Security Bible,* 2nd Edition, and *Insider Threat*. Eric is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is the founder and an executive leader at Secure Anchor Consulting, where he provides leading-edge cybersecurity consulting services, expert witness work, and leads research and development initiatives to advance the state-of-the-art in information systems security. Dr. Cole is actively involved with the SANS Technology Institute (STI). He is a SANS faculty Fellow who works with students, teaches, and develops and maintains courseware.

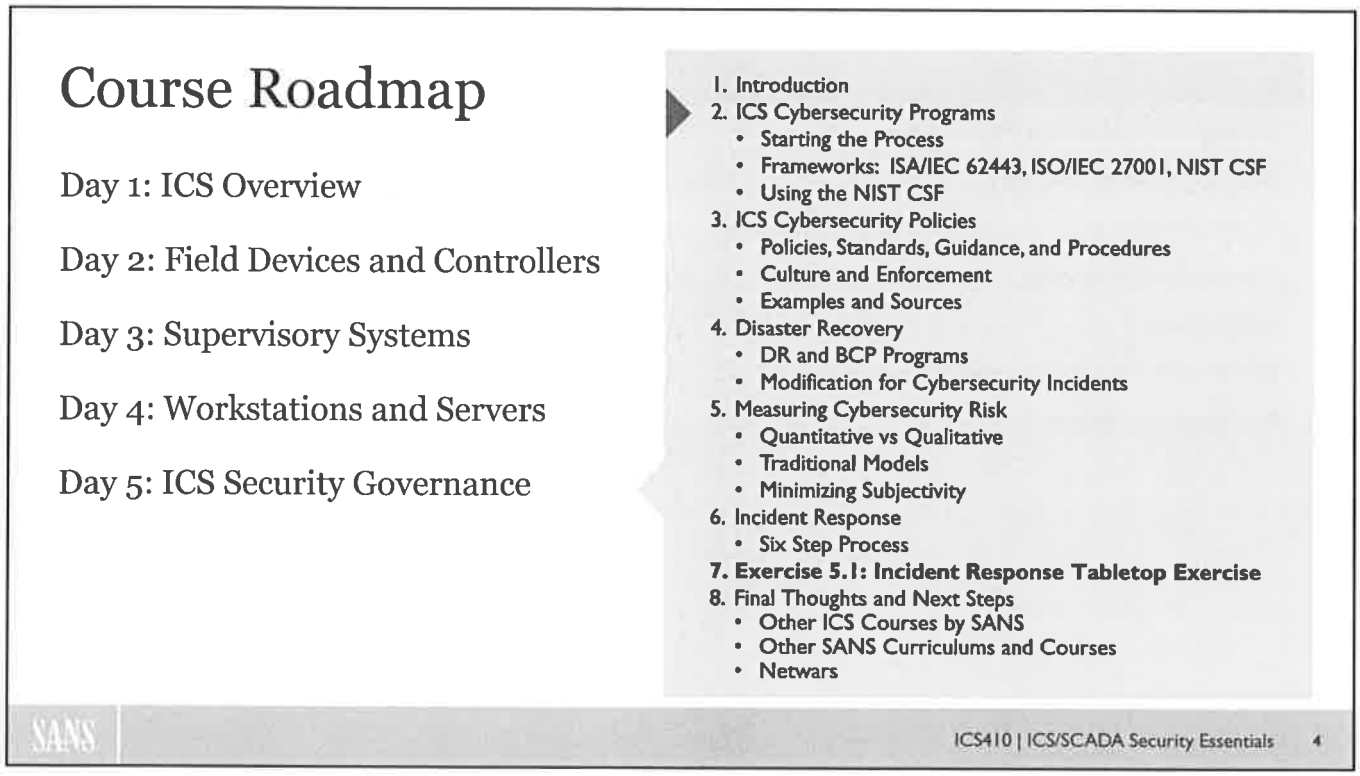
Eric Cornelius is the Director of Critical Infrastructure and Industrial Control Systems (ICS) at Cylance, Inc. He is responsible for the thought leadership, architecture, and consulting implementations for the company. His leadership keeps organizations safe, secure, and resilient against advanced attackers. Previously, Eric served as the Deputy Director and Chief Technical Analyst for the Control Systems Security Program at the US Department of Homeland Security. As an active researcher in the field of cybersecurity since 2002, Eric supported many "boots-on-the-ground" engagements involving penetration testing, forensics, and malware analysis. Through these engagements, he aided multiple government, military, and private sector organizations in protecting their networks and industrial control systems. In addition to his years of technical leadership, Eric literally wrote the book on incident response in the ICS arena. Eric's extensive knowledge of critical infrastructure and those who attack it will be brought to bear at Cylance as he leads a team of experts in securing America's critical systems.

Contributing Authors

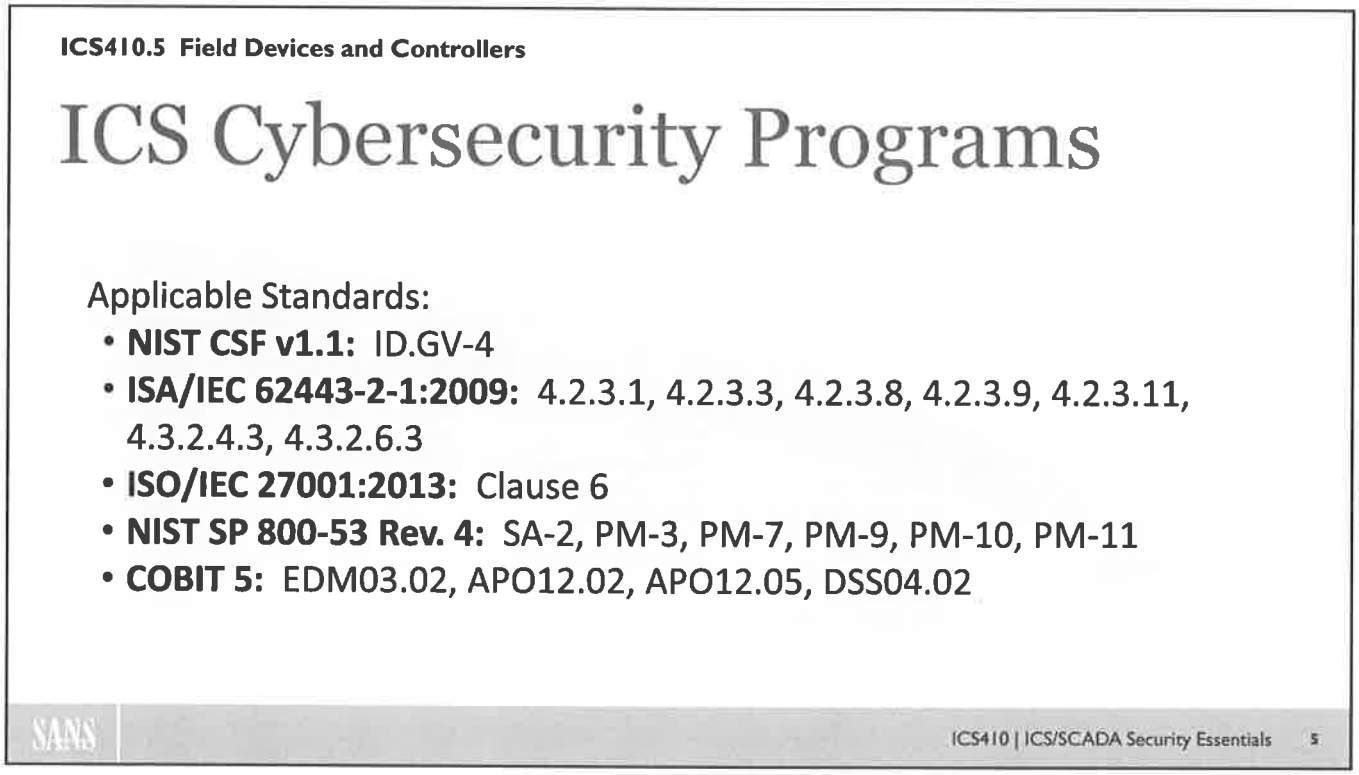
Michael Assante is currently the SANS project lead for Industrial Control System (ICS) and Supervisory Control and Data Acquisition (SCADA) security. He served as Vice President and Chief Security Officer of the North American Electric Reliability Corporation (NERC), where he oversaw industry-wide implementation of cybersecurity standards across the continent. Prior to joining NERC, Michael held a number of high-level positions at Idaho National Labs and he served as Vice President and Chief Security Officer for American Electric Power. His work in ICS security has been widely recognized and he was selected by his peers as the winner of *Information Security Magazine's* security leadership award for his efforts as a strategic thinker. The RSA 2005 Conference awarded him its outstanding achievement award in the practice of security within an organization. He has testified before the US Senate and House and was an initial member of the Commission on Cyber Security for the 44th Presidency. Prior to his career in security, Michael served in various naval intelligence and information warfare roles and he developed and gave presentations on the latest technology and security threats to the Chairman of the Joint Chiefs of Staff, Director of the National Security Agency, and other leading government officials. In 1997, he was honored as a Naval Intelligence Officer of the Year.

Tim Conway is currently the Technical Director of ICS and SCADA programs at SANS. He is responsible for developing, reviewing, and implementing technical components of the SANS ICS and SCADA product offerings. He was formerly the Director of CIP Compliance and Operations Technology at Northern Indiana Public Service Company (NIPSCO) where he was responsible for Operations Technology, NERC CIP Compliance, and the NERC training environments for the operations departments within NIPSCO Electric. Tim was previously an EMS Computer Systems Engineer at NIPSCO for eight years, with responsibility over the control system servers and the supporting network infrastructure. He previously served as the Chair of the RFC CIPC, is the current Chair of the NERC CIP Interpretation Drafting Team, a current member of the NESCO advisory board, the current Chair of the NERC CIPC GridEx 2013 Working Group, and the current Chair of the NBISE Smart Grid Cyber Security panel.

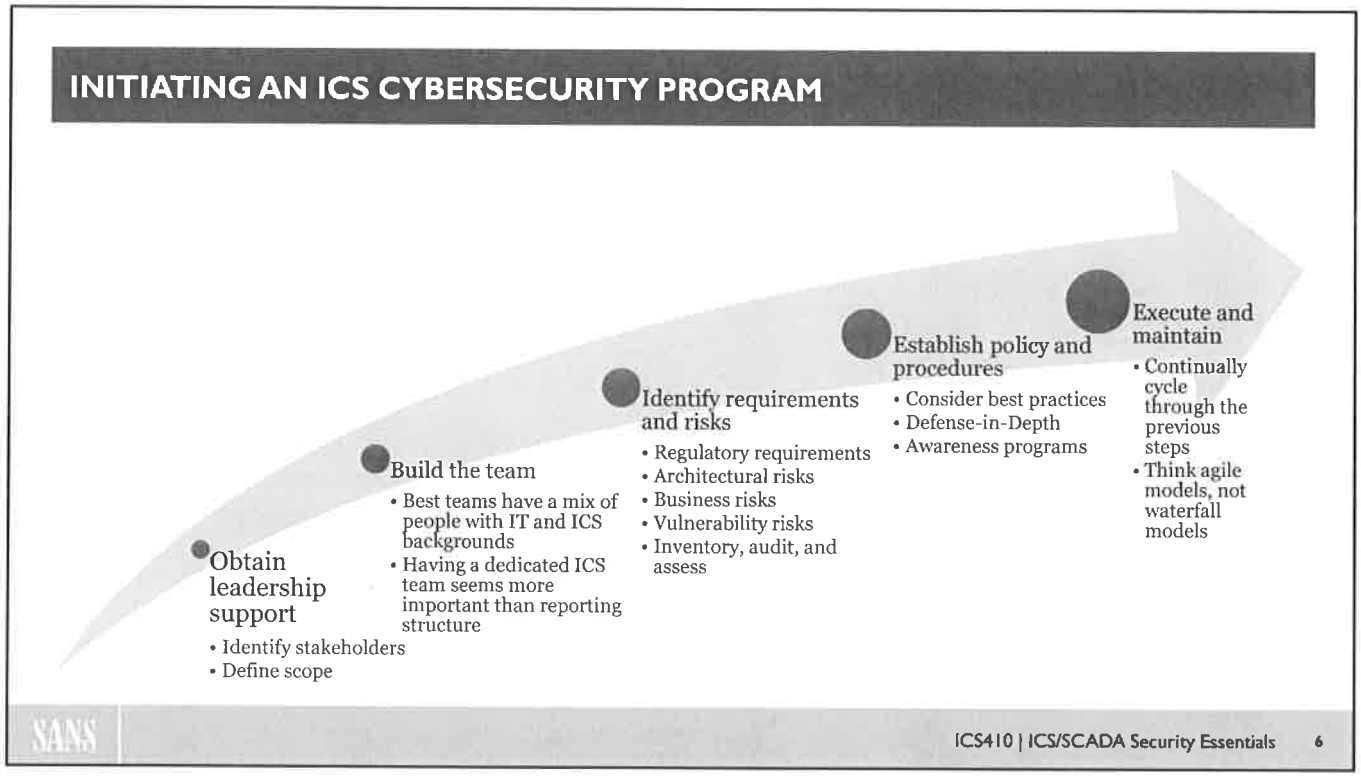
This page intentionally left blank.



This page intentionally left blank.



This page intentionally left blank.



There are many steps in initiating an ICS Cybersecurity Program in your company. The first will be getting support from leadership for funding and authority to enforce. Next, you will want to start building your ICS Cybersecurity Team. Once the team is up and running, at least with a few members, you will need to start identifying what business regulatory requirements you are required to fulfill and what cybersecurity risks your company faces. This is not an easy process and, in truth, never really ends.

Start small and organically, address it as bite-sized chunks, and continue growing your understanding of the risks you face. A good parallel is the differences in agile development compared to waterfall development. Choose small milestones that can be accomplished in weeks, not months. As you begin to understand the risks you face, start to develop and later modify your policies and procedures to address your current understandings of risk, and execute those policies and procedures in your organizations.

Manifesto for Agile Software Development's 12 principles, which apply well to cybersecurity programs:

1. Customer satisfaction by early and continuous delivery of valuable software
2. Welcome changing requirements, even in late development
3. Working software is delivered frequently (weeks rather than months)
4. Close, daily cooperation between business people and developers
5. Projects are built around motivated individuals, who should be trusted
6. Face-to-face conversation is the best form of communication (co-location)
7. Working software is the primary measure of progress
8. Sustainable development, able to maintain a constant pace
9. Continuous attention to technical excellence and good design
10. Simplicity—the art of maximizing the amount of work not done—is essential
11. Best architectures, requirements, and designs emerge from self-organizing teams
12. Regularly, the team reflects on how to become more effective, and adjusts accordingly

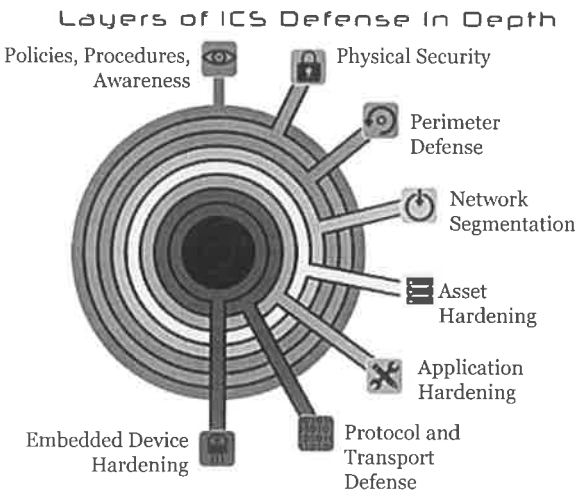
Reference:
https://en.wikipedia.org/wiki/Agile_software_development

DEFENSE-IN-DEPTH

There is no magic solution when it comes to cybersecurity

- Any layer of protection might fail
- Multiple levels must be deployed
- Must be across a wide range of controls
- Integrated Defense-in-Depth

Prevention is ideal,
but detection is a must;
however, detection without response has minimal value



ICS security requires a comprehensive, integrated approach in which multiple solutions are tiered together to accomplish a goal. There is no single security solution that will make an organization and its control systems secure because any single measure could be bypassed (and miss an attack altogether) or compromised. When protecting any entity – take the President, for example – there are many people, measures, and systems put in place to keep him secure. The same robust approach needs to be applied to your network or any critical asset in your organization.

When it comes to ICS security, there is no silver bullet. Multiple measures that complement each other must be put in place across a variety of control options. For example, you would deploy a preventive measure such as a firewall, a detective measure such as an IDS, and a deterrent measure such as a guard at your front gate, just to name a few. Even if one of the measures failed, the other measures would be able to detect the attack before there was a problem; or, catch an attack in action to minimize the amount of damage caused.

COMMON CYBERSECURITY FRAMEWORKS IN ICS

Frameworks help us go about this in a organized method

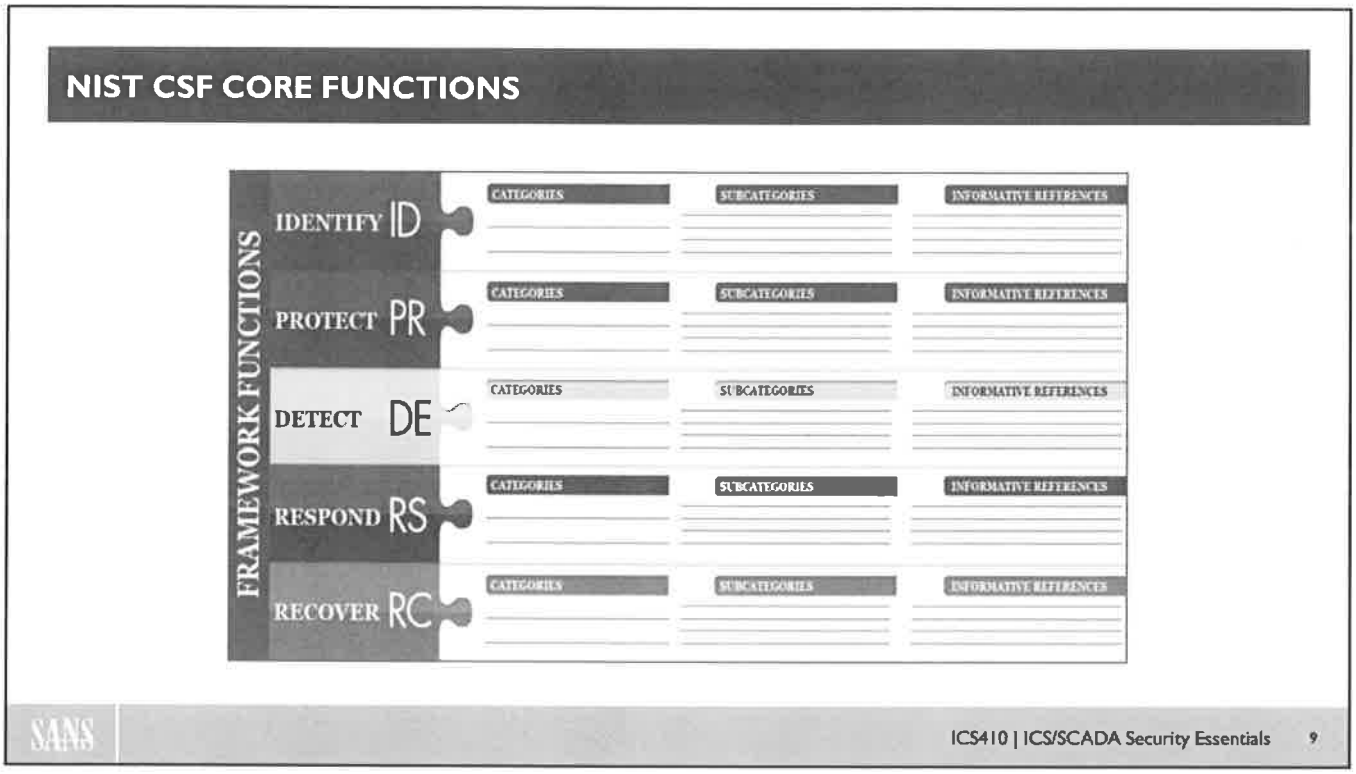
Three most-implemented frameworks are

- ISA/IEC 62443
- ISO 27001
- NIST CSF (Cybersecurity Framework)

We'll look at NIST CSF

- It is the only one that is available without cost
- Has industry-specific implementation guides
- Has over 30% adoption in North America
- Is being used in Japan, Philippines, Italy, and other countries

Resources:
https://www.nist.gov/cyberframework



From the NIST CSF:

Identify – Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include: Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

Protect – Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. The Detect Function enables timely discovery of cybersecurity events. Examples of outcome Categories within this Function include: Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. The Respond Function supports the ability to contain the impact of a potential cybersecurity incident. Examples of outcome Categories within this Function include: Response Planning, Communications, Analysis, Mitigation, and Improvements.

Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. The Recover Function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident. Examples of outcome Categories within this Function include: Recovery Planning, Improvements, and Communications.

Reference:
https://www.nist.gov/cyberframework

NIST CSF IDENTIFY (ID) FUNCTION

ID.AM – Asset Management
- Inventory of assets, map data flows, prioritize assets, and establish workforce roles

ID.BE – Business Environment
- Identify supply chains, ICS sector, organization mission, and requirements for critical services

ID.GV – Governance
- Establish security policy, information security roles/responsibilities, risk management process

ID.RA – Risk Assessment
- Identify threat/vuln sources, current threats/vulns, potential risk/impact, and risk responses

ID.RM – Risk Management Strategy
- Establish risk management process and organization's risk tolerance

ID.SC – Supply Chain Risk Management (new to 1.1)
- Identify suppliers/partners and execute contracts, assessments, and response/recovery testing

From the NIST CSF:

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

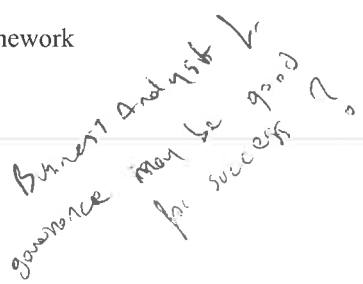
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

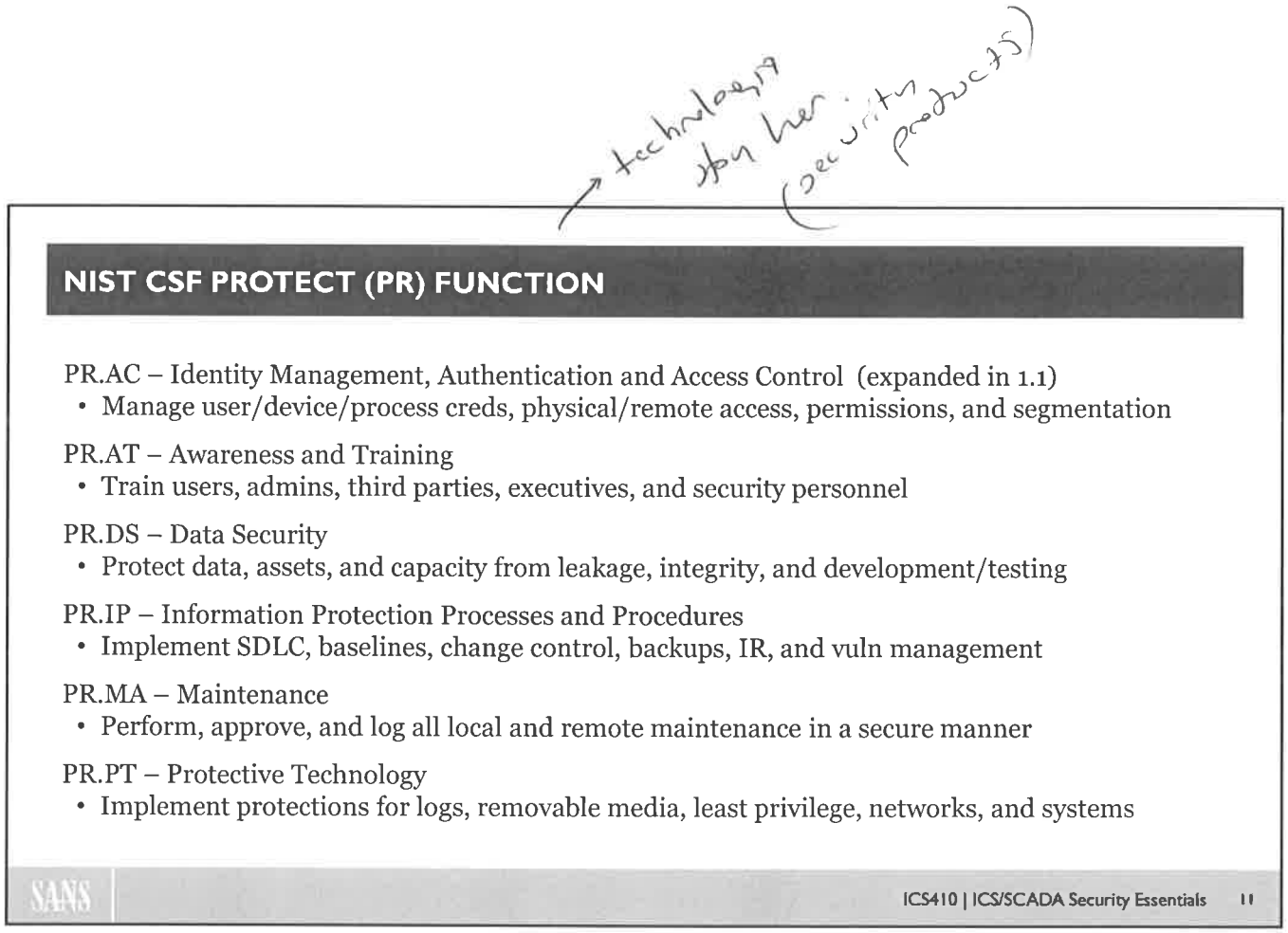
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.

Reference:
https://www.nist.gov/cyberframework





From the NIST CSF:

Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security–related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Reference:
https://www.nist.gov/cyberframework

NIST CSF DETECT (DE) FUNCTION

DE.AE – Anomalies and Events
- Collect, correlate, baseline, and analyze data flows and events
- Use multiple sources and sensors
- Establish incident thresholds

DE.CM – Security Continuous Monitoring
- Monitor for malicious activity in network, physical spaces, user actions, devices, software
- Perform vulnerability scans

DE.DP – Detection Processes
- Define detection roles, activities, and communications
- Test detection processes
- Continuously improve detection capabilities

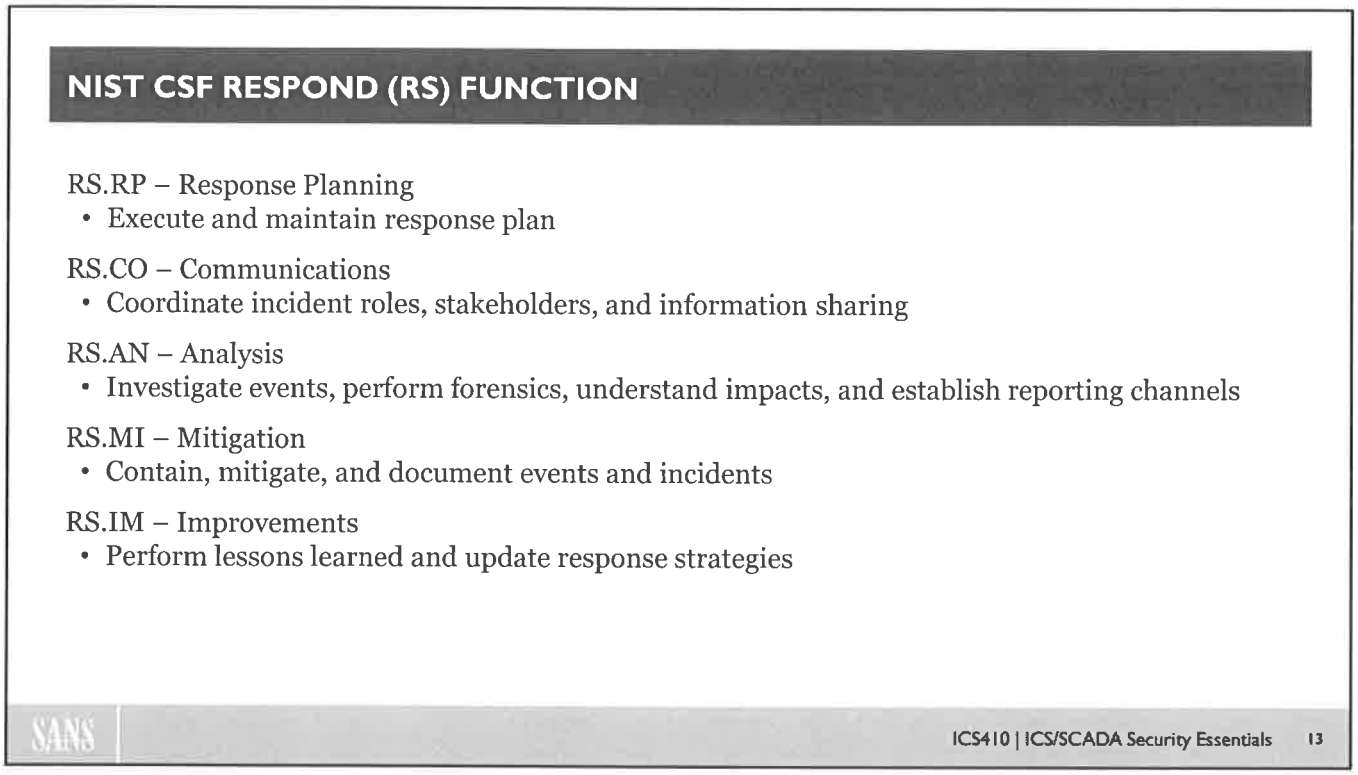
From the NIST CSF:

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Reference:
https://www.nist.gov/cyberframework



From the NIST CSF:

Response Planning (RS.RP): Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.

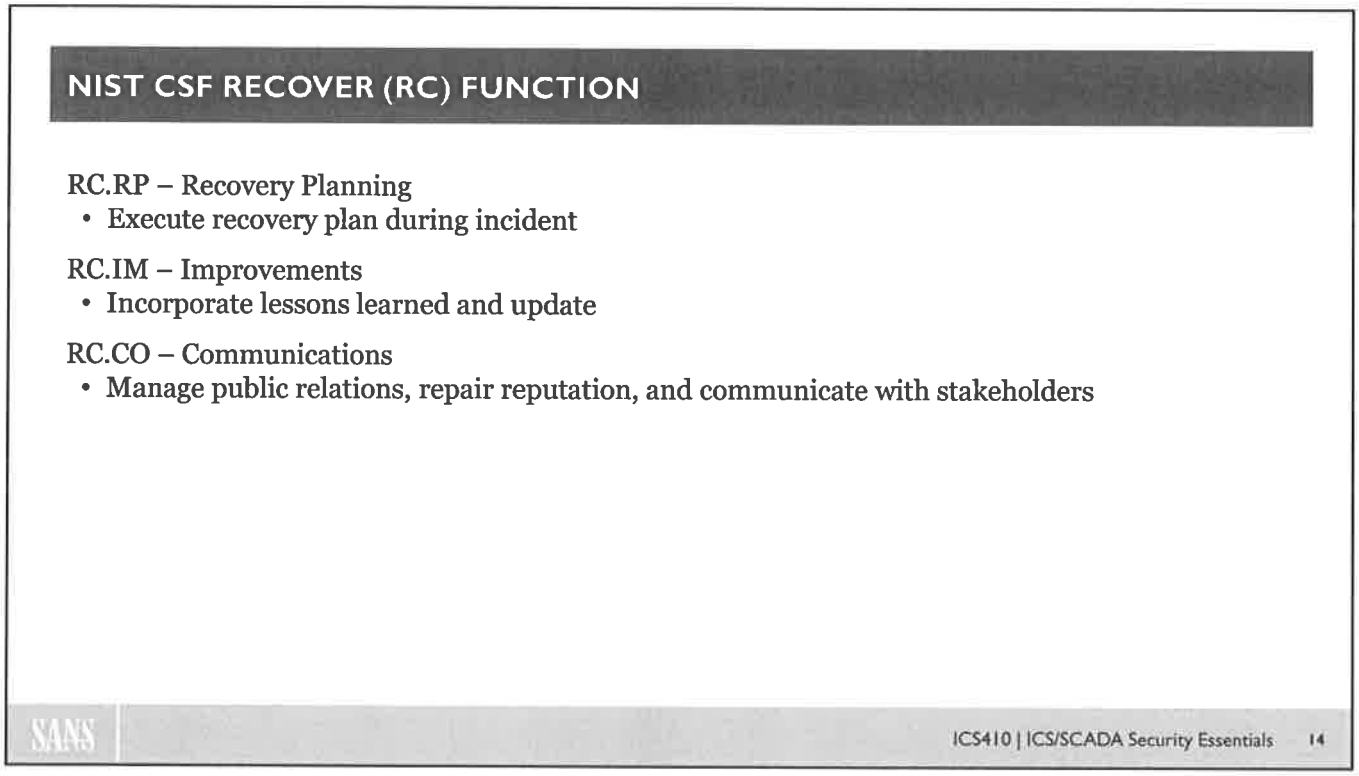
Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Analysis (RS.AN): Analysis is conducted to ensure adequate response and to support recovery activities.

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Reference:
https://www.nist.gov/cyberframework



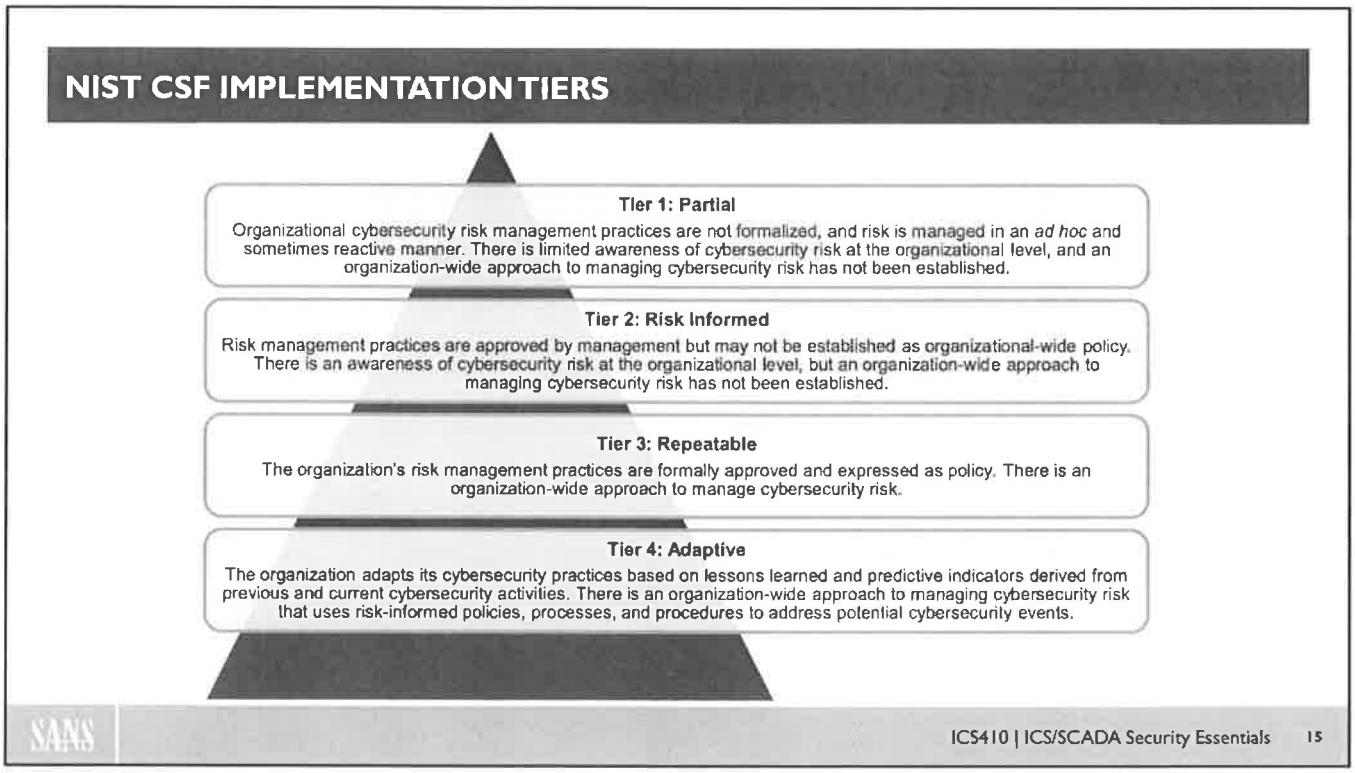
From the NIST CSF:

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

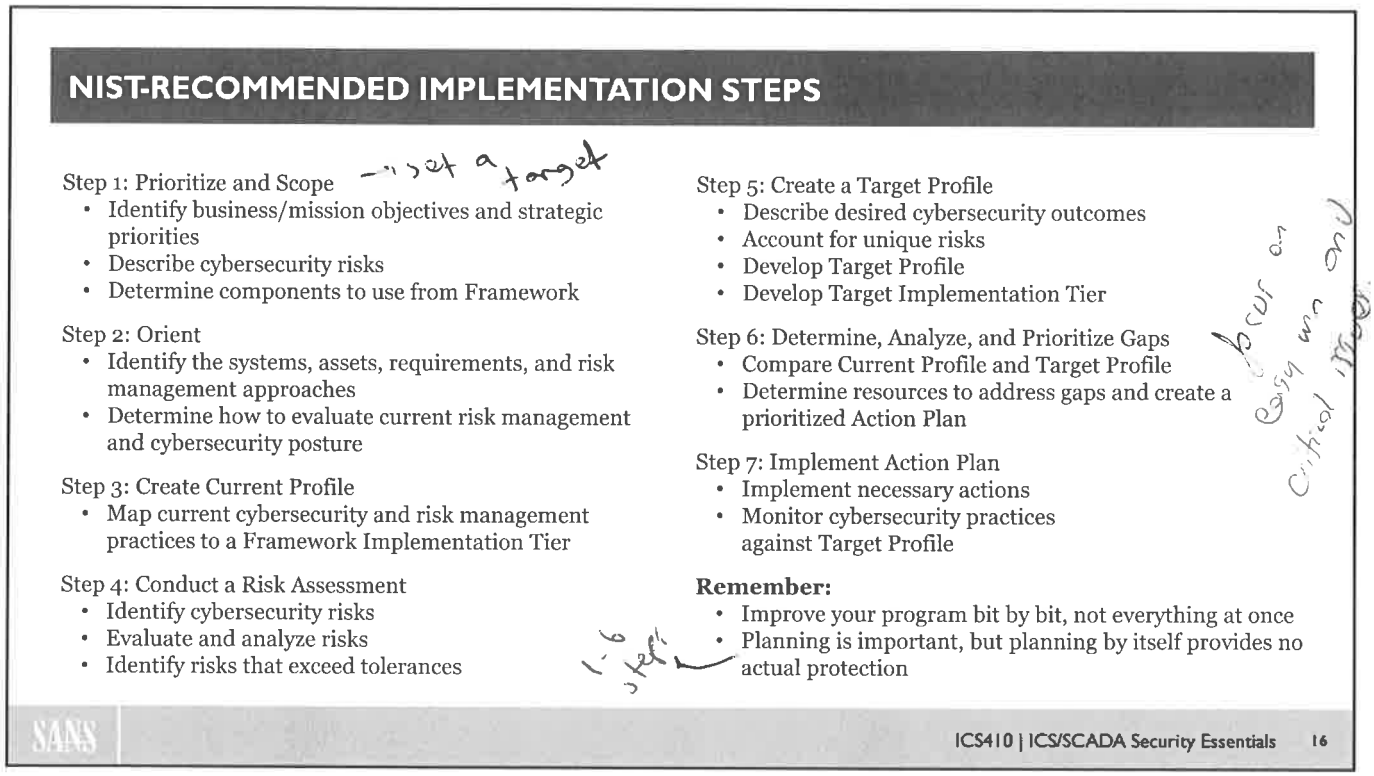
Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.

Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.

Reference:
https://www.nist.gov/cyberframework



From the NIST CSF:
The Framework Implementation Tiers ("Tiers") provide context on how an organization views cybersecurity risk and the processes in place to manage that risk. Ranging from Partial (Tier 1) to Adaptive (Tier 4), Tiers describe an increasing degree of rigor and sophistication in cybersecurity risk management practices. They help determine the extent to which cybersecurity risk management is informed by business needs and is integrated into an organization's overall risk management practices. Risk management considerations include many aspects of cybersecurity, including the degree to which privacy and civil liberties considerations are integrated into an organization's management of cybersecurity risk and potential risk responses.
The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, information-sharing practices, business/mission objectives, supply chain cybersecurity requirements, and organizational constraints. Organizations should determine the desired Tier, ensuring that the selected level meets the organizational goals, is feasible to implement, and reduces cybersecurity risk to critical assets and resources to levels acceptable to the organization. Organizations should consider leveraging external guidance obtained from federal government departments and agencies, Information Sharing and Analysis Centers (ISACs), Information Sharing and Analysis Organizations (ISAOs), existing maturity models, or other sources to assist in determining their desired Tier.
While organizations identified as Tier 1 (Partial) are encouraged to consider moving toward Tier 2 or greater, Tiers do not necessarily represent maturity levels. Tiers are meant to support organizational decision-making about how to manage cybersecurity risk, as well as which dimensions of the organization are higher priority and should receive additional resources. Progression to higher Tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.
Successful implementation of the Framework is based upon achieving the outcomes described in the organization's Target Profile(s) and not upon Tier determination. Still, Tier selection and designation naturally affect Framework Profiles. The Tier recommendation by business/process level managers, as approved by the senior executive level, will help set the overall tone for how cybersecurity risk will be managed within the organization, and should influence prioritization within a Target Profile and assessments of progress in addressing gaps.
Reference:
https://www.nist.gov/cyberframework



These steps illustrate how you can use the NIST CSR Framework to create an ICS Cybersecurity Program in you organization, or improve your current program.

Remember, start with bite-sized chunks, improving your program bit by bit. Most of us are working with teams that are understaffed and underfunded, and the worst thing you can do is attempt to do everything at once, which often results in lots of planning but little execution. The purpose of your program is to make your systems more secure, and while planning is a very necessary part of this process, planning by itself results in no actual protection.

Reference:
https://www.nist.gov/cyberframework

TAKEAWAYS AND RECOMMENDATIONS

Section takeaways

more ICS specific

- Three major frameworks: ISA/IEC 62443, ISO 27001, and NIST CSF
- Each provide a road map for improvement

Recommendations to owner/operators

- Choose a framework and iterate through it monthly
- Focus on frequent little changes instead of long monolithic changes

Recommendations to vendors

- Map your product features for all three frameworks
- Identify missing features recommended by frameworks

there will be gap. You need to fill them for a perfect security

This page intentionally left blank.

Course Roadmap

Day 1: ICS Overview

Day 2: Field Devices and Controllers

Day 3: Supervisory Systems

Day 4: Workstations and Servers

Day 5: ICS Security Governance

1. Introduction
2. ICS Cybersecurity Programs
   - Starting the Process
   - Frameworks: ISA/IEC 62443, ISO/IEC 27001, NIST CSF
   - Using the NIST CSF
3. ICS Cybersecurity Policies
   - Policies, Standards, Guidance, and Procedures
   - Culture and Enforcement
   - Examples and Sources
4. Disaster Recovery
   - DR and BCP Programs
   - Modification for Cybersecurity Incidents
5. Measuring Cybersecurity Risk
   - Quantitative vs Qualitative
   - Traditional Models
   - Minimizing Subjectivity
6. Incident Response
   - Six Step Process
7. **Exercise 5.1: Incident Response Tabletop Exercise**
8. Final Thoughts and Next Steps
   - Other ICS Courses by SANS
   - Other SANS Curriculums and Courses
   - Netwars

This page intentionally left blank.

ICS410.5 Field Devices and Controllers

ICS Cybersecurity Policies

Applicable Standards:

- **NIST CSF v1.1:** ID.GV-1
- **ISA/IEC 62443-2-1:2009:** 4.3.2.6
- **ISO/IEC 27001:2013:** A.5.1.1
- **NIST SP 800-53 Rev. 4:** controls from all families
- **CIS CSC:** 19
- **COBIT 5:** APO01.03, APO13.01, EDM01.01, EDM01.02

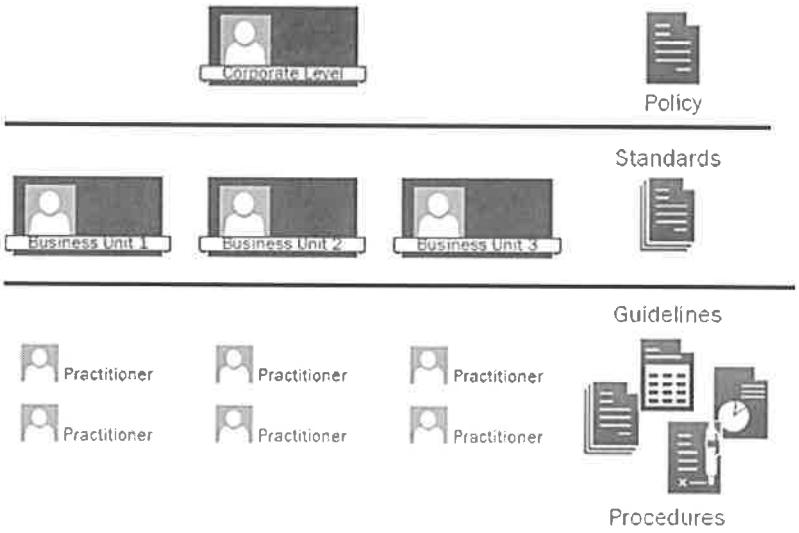
This page intentionally left blank.

NERC CIP → best (baseline) compliance work with critical infrastructure.

POLICY HIERARCHY

Policies are comprised of different types of documents or sections

- Policies: High-level directives
- Standards: Mid-low-level directives
- Guidelines: Low-level recommendations and examples
- Procedures: Low-level steps and checklists



In the example organization implementation picture, you can see policies and their association to the highest levels of an organization and the use of standards by management across various business units. The guidelines and procedures are implemented by the practitioner levels in the organization.

We will now discuss the uniqueness of each document type and why they are utilized.

POLICY

A high-level corporate-supported document that details business goals and objectives

Policies typically

it must be applied universally

- Apply to all personnel including contractors and vendors
- Nonperformance of a policy item typically results in disciplinary action up to and including termination
- Are goal-oriented
- Are supported by standards, guidelines, and procedures

Policies are typically viewed as a governing document that refers to standards, guidelines, and procedures. Sometimes multiple standards, guidelines, and procedures exist to support a governing policy. Policies help shape the culture of an organization and focus on the mission or goals of the organization and not on the journey or steps necessary to achieve the desired goal.

Policies are all-encompassing in that they typically apply to all individual employees, contractors, and vendors. Basically, anyone who is being paid by an organization is subject to the policy, and nonperformance of a policy item will typically result in disciplinary action up to and including termination.

STANDARD

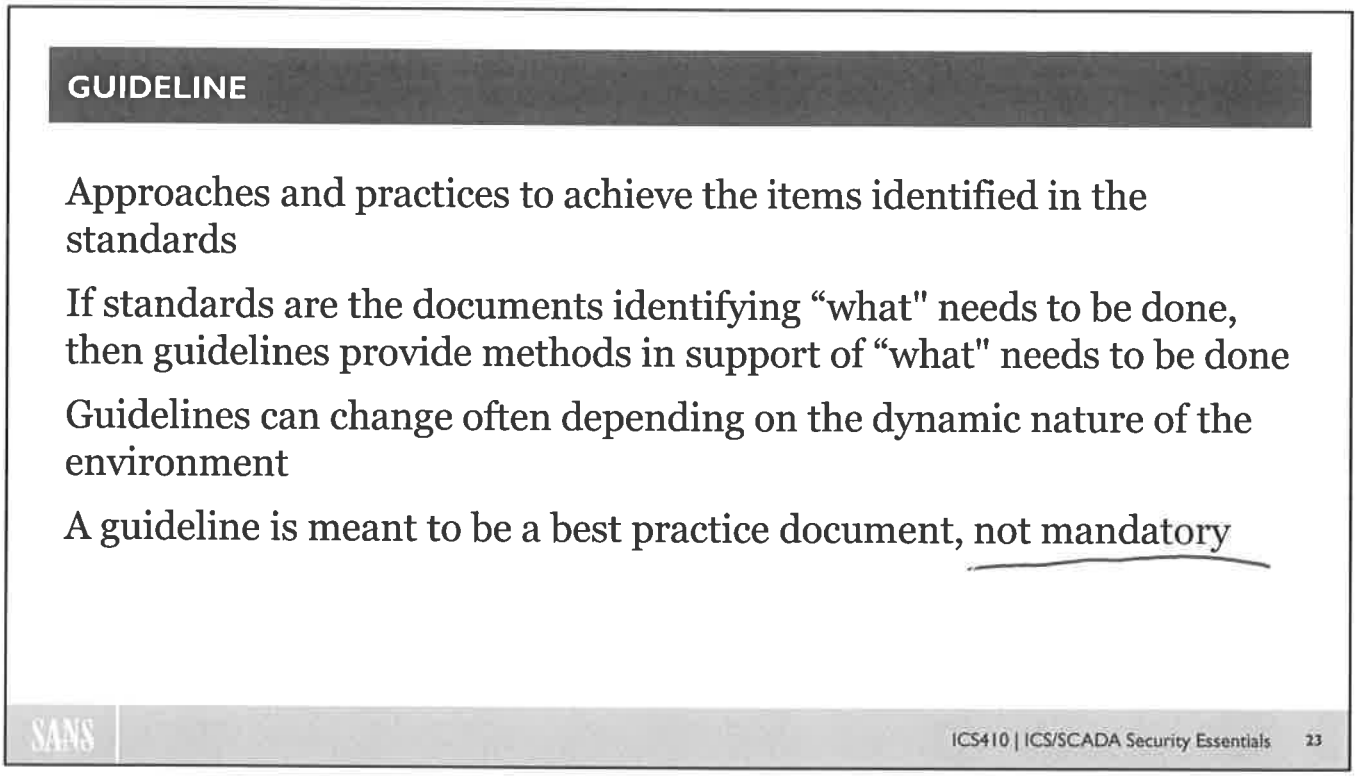
A set of requirements or framework that provides guidance on what must be done to support the policy

Standards can differ among specific business units with details or approved exemptions depending on the business unit's specific needs

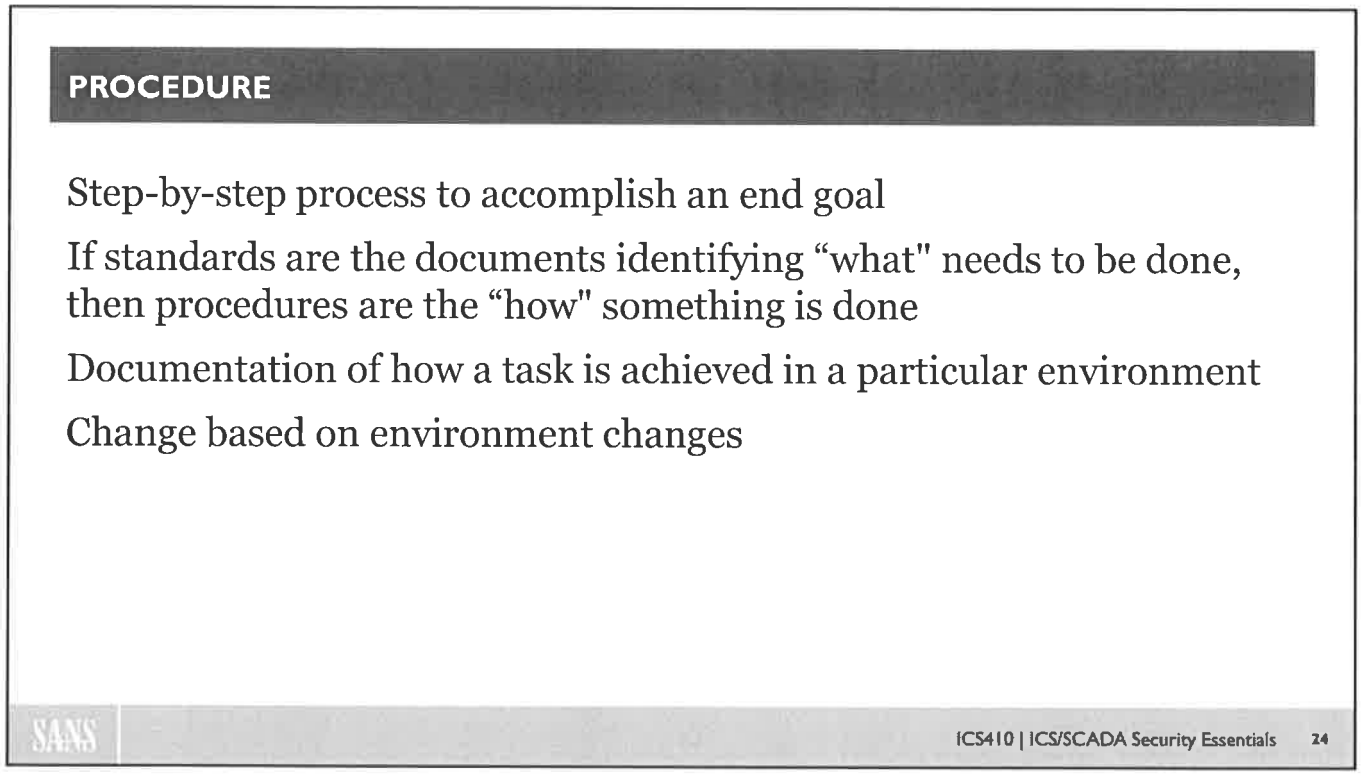
Specific standards can exist for specific business use: Company phone standard, laptop standard, desktop standard, email standard, regulation-specific standard, etc.

Standards should set requirements that can be met at least 90% of the time
- Change scope to meet the 90% rule of thumb
- Or demote the requirement to a guidance

Standards provide the details regarding what must be done in support of the policy. Often, standards vary within an organization based on specific business unit operating needs and may require documented exemptions to the policy. An example of this may be an exemption to the corporate policy, which explicitly allows the cybersecurity team to run specific tools on the network to capture and analyze traffic. In addition, specific standards may exist for certain business needs like company phones, laptops, desktops, and email application standards.



Guidelines exist as the most flexible document in this chain. Guidelines provide some best practice framework around how to satisfy the standards and they change depending on changes in the environment.



If you consider these documented approaches in the context of a family trip, policies indicate where the family is going; standards indicate when the family will be at a location and what will be done; guidelines would be recommendations of things to do in the area; and procedures would be the step-by-step directions for getting there.

Sans → security - resources - policy.

ELEMENTS OF A WELL-WRITTEN POLICY

An effective and realistic security policy is the key to effective and achievable security

The following need to be included in a policy

- Purpose
- Related documents or references
- Cancellation or expiration → start - end dat - to check and entil.
- Background → reason to believe
- Scope
- Policy statement

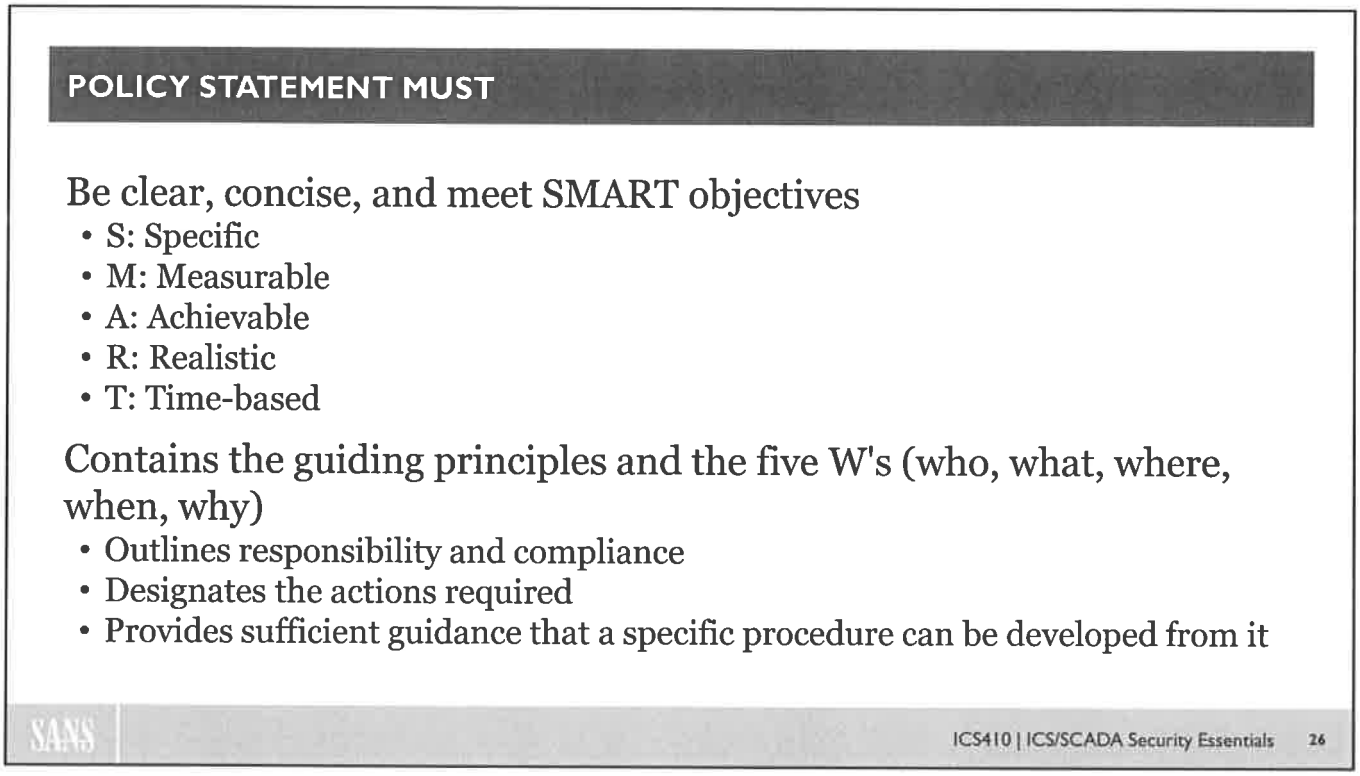
Ensure the policy has all its parts

A policy is a directive that indicates a conscious decision to follow a path toward a specified objective. Often a policy can initiate the institution and empowerment of resources or direct action by providing procedures or actions to be carried out. The policy itself should be effective and realistic and have achievable security goals.

It is critical to write down in a clear and concise manner what is expected of everyone in the organization when it comes to security. It is also helpful to inform people about what is expected of them, what the organization does, and what others in various roles within the organization do.

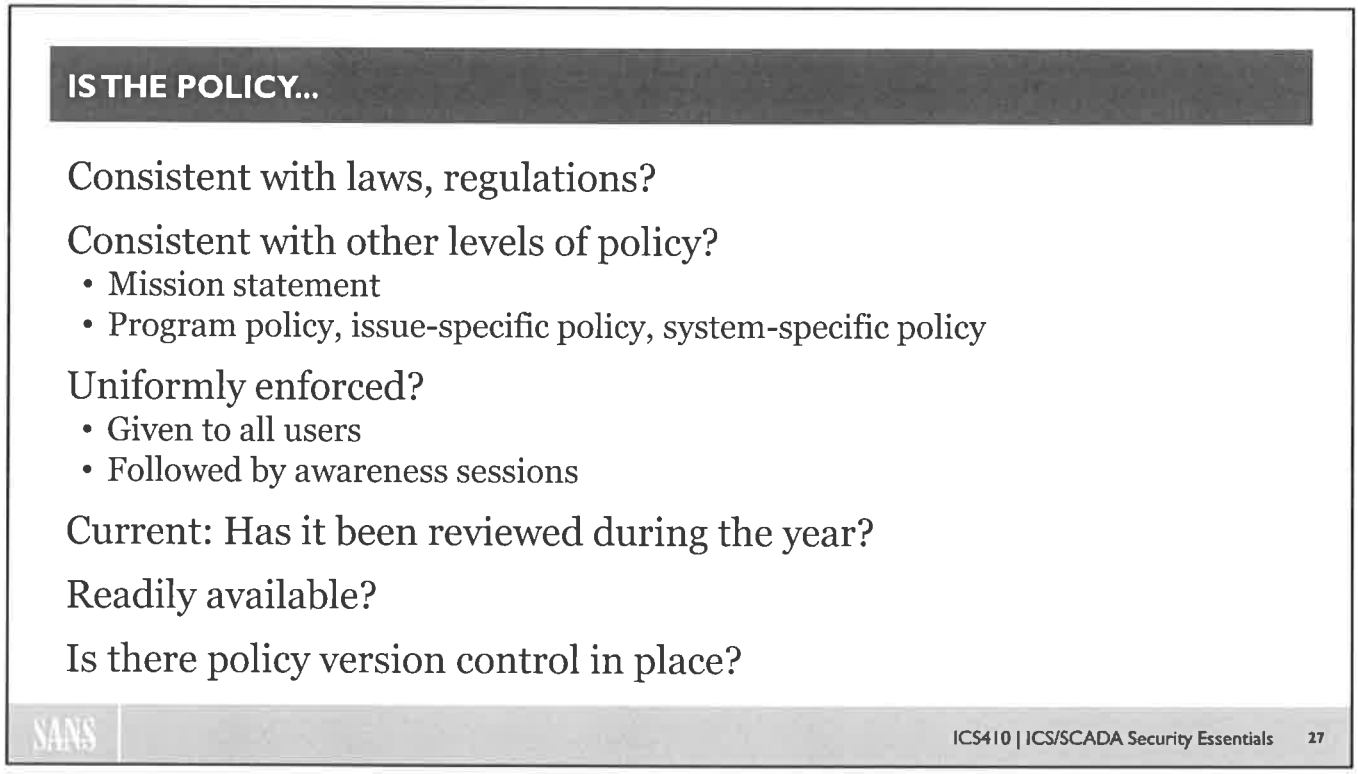
It is good to follow an approach where if the policy you need does not exist, or is badly out of date, you create, or update it, and then have it approved. The final step in establishing a framework is to assess critical policies. Even though you just wrote or updated them and you know they are correct, policies should be checked. It is better if you do not check your own work. We can only spot our own errors a small percentage of the time. When you ask a person to help you by verifying policy contents, ask that they include the most common elements in their analysis, including:

- **Purpose**: Security policy usually contains a statement, often at the beginning, describing the reason the policy is being established and any associated goals.
- **Related documents**: This is often titled "References" and usually cites higher-level policy or implementation guidance.
- **Cancellation**: New or updated policy may supersede existing (perhaps outdated) policy. This section identifies those policies and clarifies what is actually in effect.
- **Background**: This optional section provides information amplifying the need for the policy. It may also provide historical information relevant to the subject.
- **Scope**: This section identifies the depth and breadth of coverage (to whom or what the policy applies). Is it for one element of the organization or will it also apply to contractor agencies who work for your organization?
- **Policy statement**: Identifies the actual guiding principles or what is to be done. The statement(s) are designed to influence and determine decisions and actions within the scope of coverage. The statements should define actions that are prudent, expedient, or advantageous to the organization.



A great way to check your policy, is to use the SMART acronym above. Just like in setting SMART goals, creating SMART policies can be highly effective.

Policy is not detail-oriented; it is a high-level focus about who has to do what. It should not include step-by-step instructions. The rule of policy assessment is that the policy covers the "who" and "what needs to be done." Procedures cover how to do it. For example, the policy would state that each user must change his or her password every 90 days. The procedures would give you the details of how to change a password on a given operating system. In general, procedures can be updated with far less review than policy.



Security policy must also be in accordance with local, state, and federal computer-crime laws. ISMS (Information Security Management System) is a process by which an organization formulates security policy based on ISO 27001 Standards. Consider the information that needs to be secure and consider the level at which it must be secured, and then examine the policy to see whether it is consistent with the mission statement and with the following other policies:

Program policy: This high-level policy sets the overall tone of an organization's security approach. Typically, guidance is provided with this policy to enact the other types of policies and who is responsible. This policy may provide direction for compliance with industry standards such as ISO, QS, BS, AS, etc.

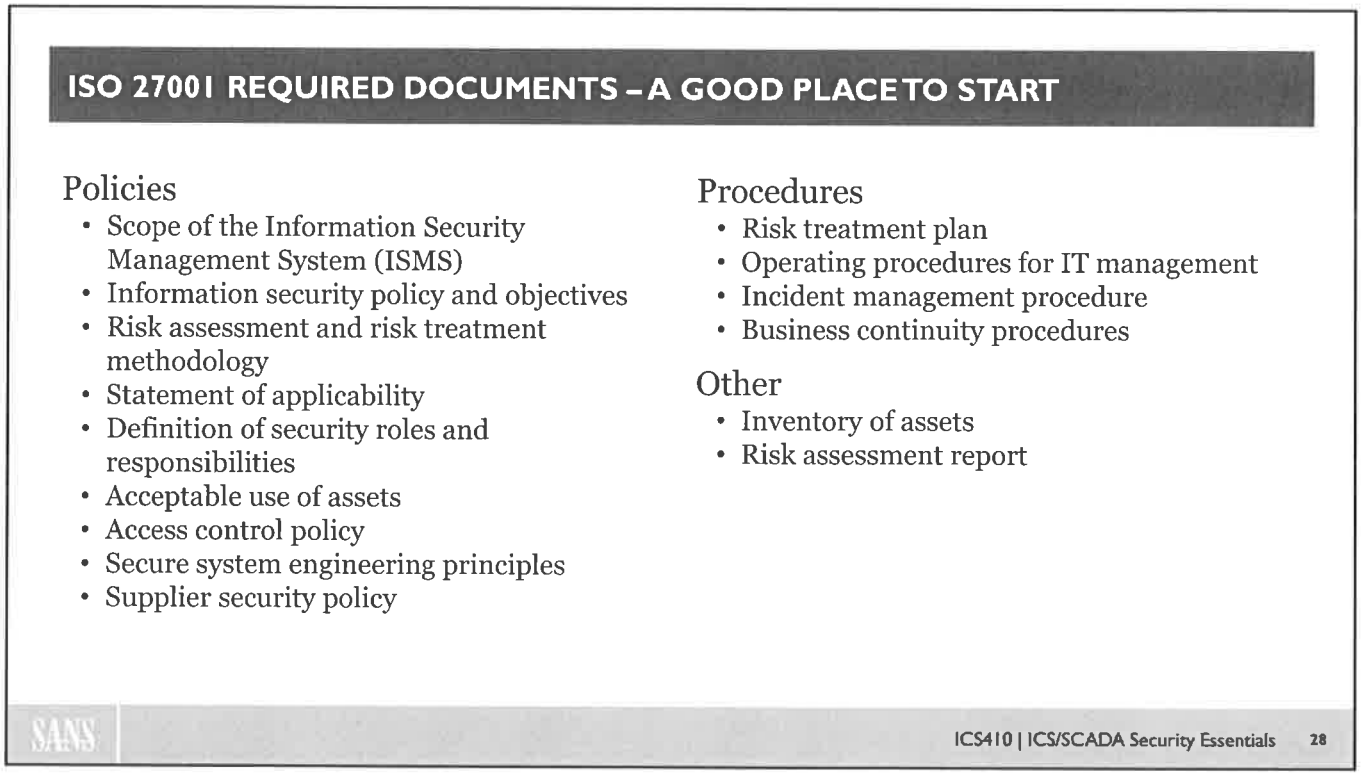
Issue-specific policy: These policies are intended to address specific needs within an organization. This may include password procedures, internet usage guidelines, and more. This is not as broad a policy category as the program policy; however, it is broader than the system-specific policy.

System-specific policy: For a given organization, there may be several systems that perform various functions where the use of one policy governing all of them may not be appropriate. It may be necessary to develop a policy directed toward each system individually. This is a system-specific policy.

If you discover any discrepancies, note them because you will need to resolve them for the policy to be meaningful.

Again, note any contradictions you discover so that you can get the document corrected.

Examine the policy for provisions to keep it current. Security policy should be reviewed regularly. Policy revisions should reflect lessons learned from recent incidents and new threats to the organization's security.



ISO 27001 is a good source to consult for which policies and procedures you need to have as part of your ICS Cybersecurity Program. ISO 27001:2013 requires the following documents.

Policies

- Scope of the Information Security Management System (4.3)
- Information security policy and objectives (5.2 and 6.2)
- Risk assessment and risk treatment methodology (6.1.2)
- Statement of applicability (6.1.3 d)
- Definition of security roles and responsibilities (A.7.1.2 and A.13.2.4)
- Acceptable use of assets (A.8.1.3)
- Access control policy (A.9.1.1)
- Secure system engineering principles (A.14.2.5)
- Supplier security policy (A.15.1.1)

Procedures

- Risk treatment plan (6.1.3 e and 6.2)
- Operating procedures for IT management (A.12.1.1)
- Incident management procedure (A.16.1.5)
- Business continuity procedures (A.17.1.2)

Other

- Inventory of assets (A.8.1.1)
- Risk assessment report (8.2)

ISO 27001 ADDITIONAL RECOMMENDED DOCUMENTS

Policies

- Controls for managing records
- Bring your own device (BYOD) policy
- Mobile device and teleworking policy
- Information classification policy
- Password policy
- Disposal and destruction policy
- Clear desk and clear screen policy
- Change management policy
- Backup policy
- Information transfer policy
- Business continuity strategy

Procedures

- Procedure for document control
- Procedure for internal audit
- Procedure for corrective action
- Procedures for working in secure areas
- Exercising and testing plan
- Maintenance and review plan

Other

- Business impact analysis

ISO 27001:2013 also recommends the following documents, but does not require them. This is also sound guidance for you and your program, suggesting that you should focus on the set on the previous slide first, then move on to these documents.

Policies

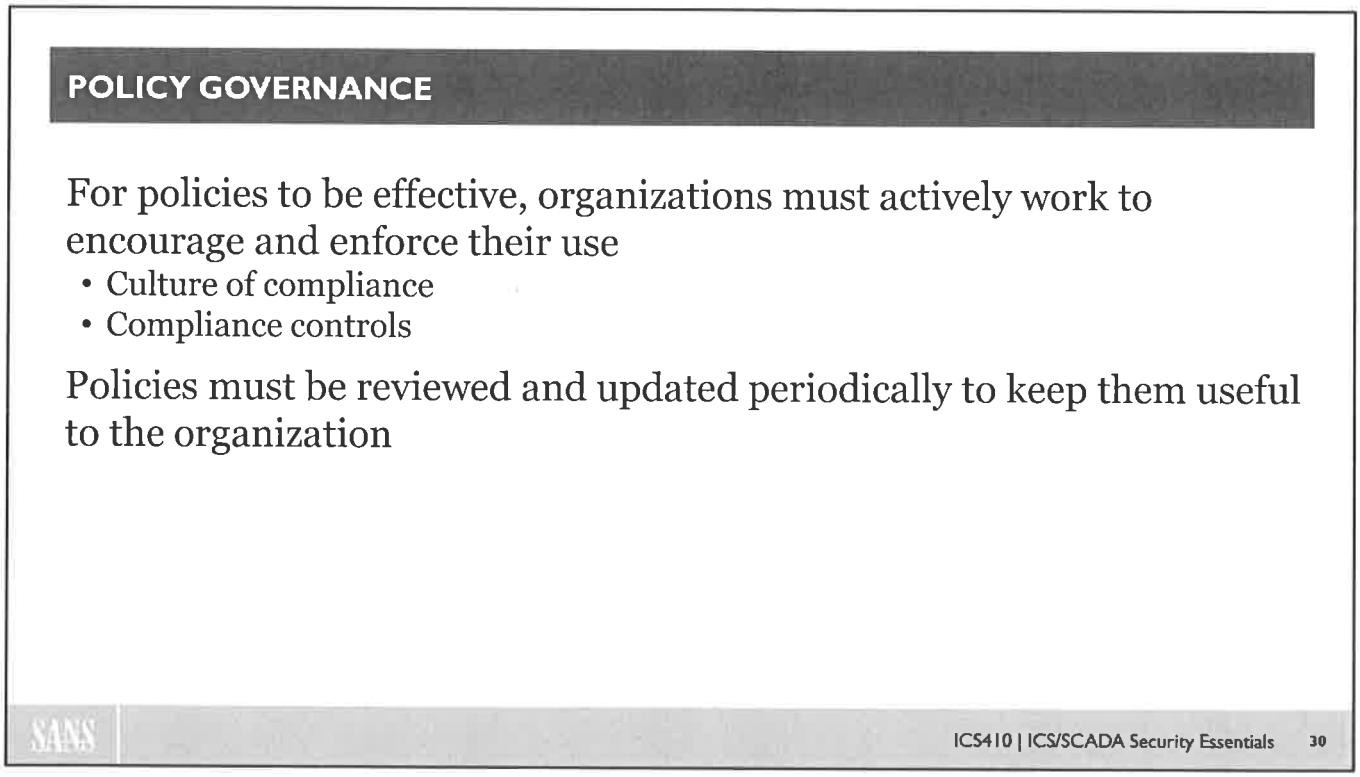
- Controls for managing records (7.5)
- Bring your own device (BYOD) policy (A.6.2.1)
- Mobile device and teleworking policy (A.6.2.1)
- Information classification policy (A.8.2.1, A.8.2.2, and A.8.2.3)
- Password policy (A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, and A.9.4.3)
- Disposal and destruction policy (A.8.3.2 and A.11.2.7)
- Clear desk and clear screen policy (A.11.2.9)
- Change management policy (A.12.1.2 and A.14.2.4)
- Backup policy (A.12.3.1)
- Information transfer policy (A.13.2.1, A.13.2.2, and A.13.2.3)
- Business continuity strategy (A.17.2.1)

Procedures

- Procedure for document control (7.5)
- Procedure for internal audit (9.2)
- Procedure for corrective action (10.1)
- Procedures for working in secure areas (A.11.1.5)
- Exercising and testing plan (A.17.1.3)
- Maintenance and review plan (A.17.1.3)

Other

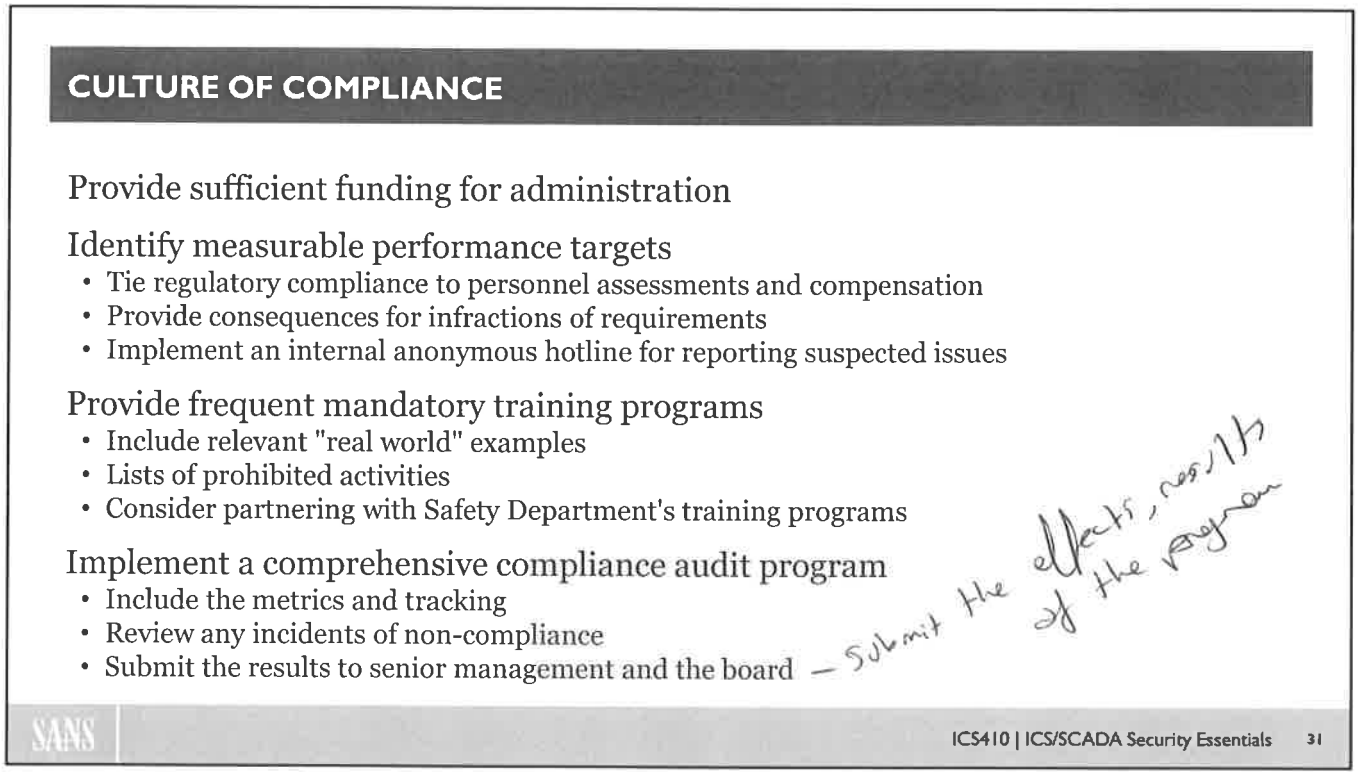
- Business impact analysis (A.17.1.1)



A well-written policy with clear, concise guidance is of relatively no use if it is not enforced and adhered to. Ensuring that a policy is actually implemented begins with an organization's culture and a widely known understanding throughout the organization that compliance is of utmost importance, which requires support throughout the organization, starting with leadership. This is typically referenced as a culture of compliance within an organization, and many organizations develop a communications approach to providing awareness of the internal compliance culture.

Organizations typically implement compliance controls to ensure that policies are being implemented effectively and to provide for routine validation that any deficiencies are being tracked and mitigated in a manner that prevents recurrence.

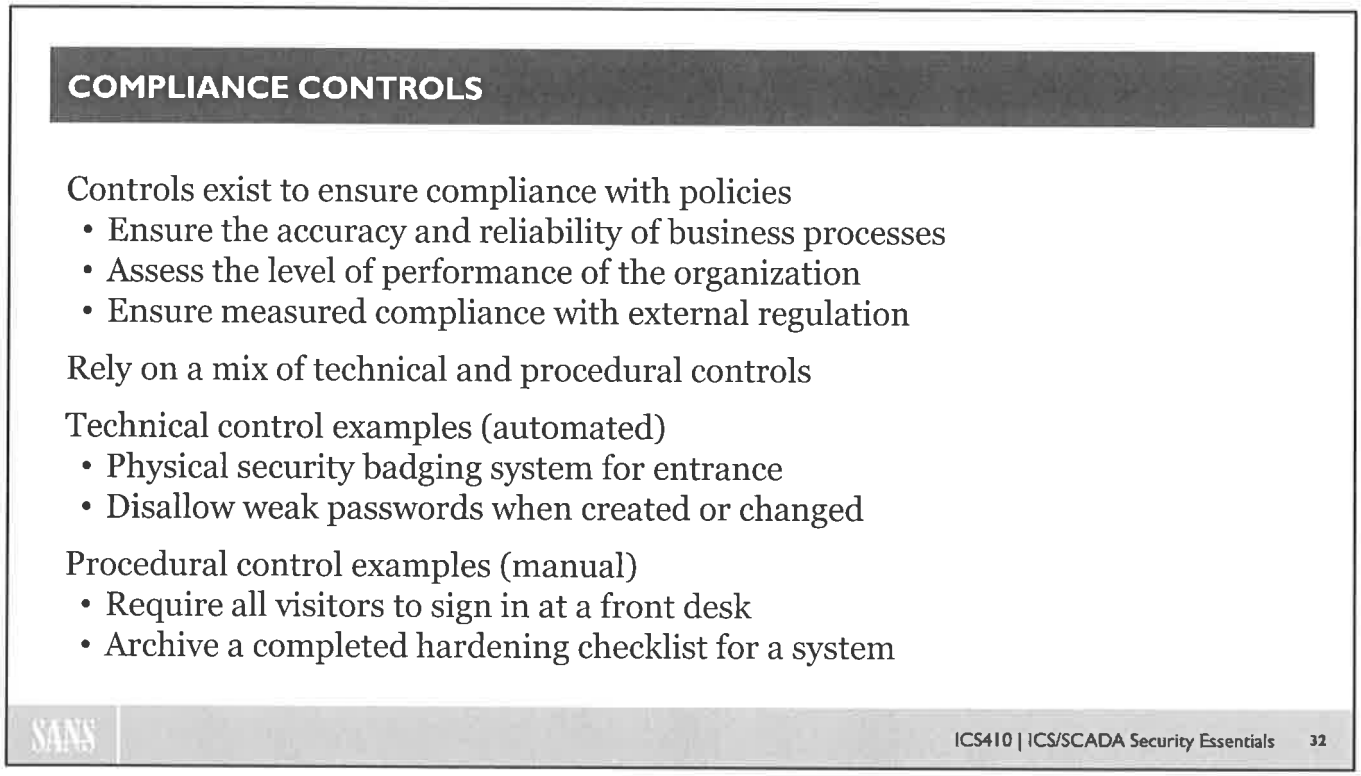
In addition to a strong culture of compliance and effective compliance controls, organizations must perform routine reviews of their policies and update them as needed. This process ensures policies reflect the current state of the business and ensures that current leadership has reviewed and understands the guidance that has been established for the organization. Compliance gap assessments can also be used to validate current performance levels compared to expected compliance-related requirements.



The US Federal Energy Regulatory Commission provided guidance through the issuance of a policy statement on compliance. Docket No. PL09-1-000 says to:

> Provide sufficient funding for the administration of compliance programs by the Compliance Officer.
> Promote compliance by identifying measurable performance targets.
> Tie regulatory compliance to personnel assessments and compensation, including compensation of management.
> Provide for disciplinary consequences for infractions of Commission requirements.
> Provide frequent mandatory training programs, including relevant "real world" examples and a list of prohibited activities.
> Implement an internal hotline through which personnel may anonymously report suspected compliance issues.
> Implement a comprehensive compliance audit program, including the tracking and review of any incidents of non-compliance, with submission of the results to senior management and the board.

Reference:
http://www.ferc.gov/whats-new/comm-meet/2008/101608/M-3.pdf



Controls provide the governance tools to ensure that policies are being complied with throughout the organization. Strong technical and procedural controls help to ensure that business processes routinely and consistently perform accurately and reliably.

When controls are used consistently, they can help build a picture or scorecard of performance across the organization to determine if there are specific areas of concern.

Controls may also be implemented to assess continued compliance to external regulation measures.

These objectives will be achieved in ICS environments through technical controls (automated processes) and through procedural controls. An example of a technical control is a physical security badging system or an electronic authentication system for cyber assets. Procedural control examples could be to require all visitors to sign in at a front desk when in a facility.

POLICY RESOURCES

Your IT department's current IT security policies
- Don't be an exception
- Duplicate what they have and modify for ICS
- Try to stay as close as you can to what they have
- Work with IT and management to modify scope between IT and ICS policies
- Highest-level policies will encompass all; mid-level should start to diverge

Other sources if you are starting from scratch, none ICS specific
- The SANS Policy Website has a great set to start with for free
  - http://www.sans.org/security-resources/policies/
- CSO Online provides security tools, templates, and policies
  - http://www.csoonline.com/article/486324/security-tools-templates-policies
- Information Shield has a complete set you can purchase
  - http://www.informationshield.com/

The best place to start is with your IT department's current IT security policies. The last thing you want as an ICS Security team is to be an exception to the formal company IT security polices. You aren't an exception—you just have different constraints and requirements. Duplicate what the IT security teams have already created and modify them for ICS. You will need to change the scope to what is appropriate for ICS, but while you do that, try to stay as close as you can to what they have. This will allow for easier company-wide updates and minimize the pushback you receive. Work with IT and management to modify scope between IT and ICS policies. This will mostly be network specific, relating to assets or data residing in ICS networks from Layers 3 and below. You should end up with your highest-level policies in the company having a scope that encompass both IT and ICS, with your mid-level and lower polices starting to diverge into separate policies.

Other resources are available for organizations to reference and utilize when developing policies from scratch. These are all non-ICS-specific policies, but remember, the reasons our ICS systems are vulnerable and most of what we do to defend them are focused around IT technologies, so our ICS policies are mostly IT focused. The templates available provides a great starting point and framework for policy development and can be a useful resource to compare against existing policies to see whether there are any gaps or areas of weakness that should be further developed.

References:
The SANS Policy Website – http://www.sans.org/security-resources/policies/
CSO Online – http://www.csoonline.com/article/486324/security-tools-templates-policies
Information Shield – http://www.informationshield.com/

REGULATORY EXAMPLES REQUIRING CYBERSECURITY POLICIES

For ICS-specific examples, look at government regulation and guidance efforts
- ISA/IEC 62443
- CPNI – UK Centre for the Protection of National Infrastructure
- NIST SP800-53 and SP800-82

North America bulk power systems are subject to the NERC Standards

North American Electric Reliability Corporation (NERC) is a not-for-profit entity
- Ensures the reliability of the BES (Bulk Electric System) in North America
- NERC has a unique enforcement capability
- Matured over the last 10 years with many updates

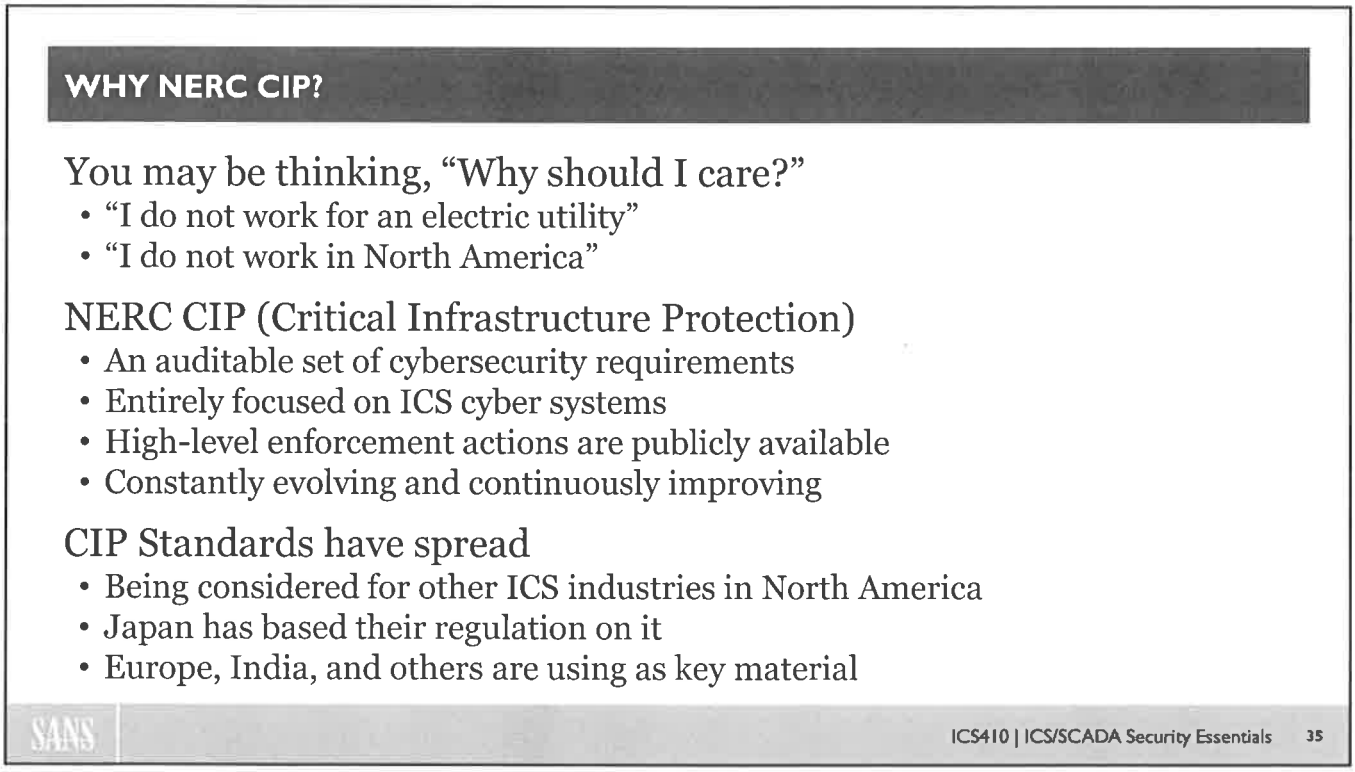
Throughout the day, we will review key examples of the NERC Standards

We are quickly covering the North America bulk power system regulatory scheme adhered to (by agreement) by the United States, Canada, and Mexico. The regulations are enforced by law and agreement in the member states and are implemented by Electric Reliability Organizations (ERO). The North American Electric Reliability Corporation (NERC) was selected as an industry body to serve as the ERO. The following slides are an example of NERC's regulation for some of the topics we have discussed. The NERC Critical Infrastructure Protection Standards (NERC CIP) were selected for a review because they are the first comprehensive cybersecurity regulation applied to the main segments of bulk power systems in three countries and have a wealth of information that can be analyzed and openly discussed. We will use this information to see where cybersecurity controls and practices have been successful and/or challenging for power ICS.

The North American Electric Reliability Corporation (NERC) is a not-for-profit entity whose mission is to ensure the reliability of the bulk power system in North America. NERC develops and enforces reliability standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico.

While other sectors have developed standards and frameworks for cybersecurity requirements for critical infrastructure, NERC has a unique enforcement capability and has matured over the last 10 years. We will look at how the enforceable NERC Standards fit for a couple of the topics we discuss.

You should look to the NERC Standards as a possible model that many sectors will eventually heed for critical infrastructure cybersecurity assets. Look to the electric sector as a possible compass for where your sector of interest may go.



The NERC CIP Standards provide a non-academic, non-research-based approach to ICS cybersecurity requirements that have been implemented by hundreds of organizations effectively over the last 10 years. The standards have never been perfect and as a result, have continued to evolve, demonstrating flexibility in providing the necessary requirement language detailing what an organization must do while remaining non-prescriptive in regard to how an organization can meet the requirement.

These improvements over time have moved the standards from the early days of the 1200 Standards, which were Control Center–focused, to the 1300 Standards, which expanded into field assets and eventually into the CIP Standards framework that has been in effect for many years. The CIP Standards should be viewed as one paradigm in the Versions 1, 2, and 3 implementations of the requirements. In this paradigm, the CIP Standards required organizations to identify the assets they owned or operated that were critical to the Bulk Electric System, and these earlier standards took an "everything gets everything" approach, where all identified Critical Cyber Assets were subject to all requirements. This earlier paradigm resulted in many unintended consequences and had numerous organizations self-identifying that they did not own or operate any critical assets. The new paradigm, partially introduced in CIP Version 4, but going into effect in CIP Versions 5 and 6, took a high, medium, and low criteria-based approach that identified assets that were critical within the standards and implemented a systematic approach to allow organizations to group assets and apply the requirements to the group of assets, rather than each individual asset.

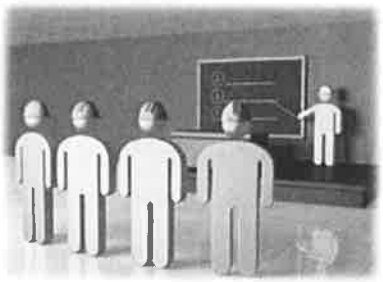
As organizations manage their CIP programs, they undergo audits and potential penalties for areas of non-compliance. This violation information is publicly available and can be evaluated to determine the areas of greatest challenge within the CIP Standards, as well as evaluating the areas of greatest risk for an adversary to target. The violation information for CIP-related penalties does not provide the details of which organization received the penalty, but the details of the non-compliance event are provided. Defenders in many industries can learn from these challenges.

Throughout North America, the NERC CIP Standards have been evaluated for applicability, adoption, or modification to apply similar requirements on other critical infrastructure, such as water, oil, and gas. In addition, other countries have conducted studies and evaluated the NERC CIP Standards during the development of their country- or region-specific guidance.

NERC REGULATION ENFORCEMENT STRUCTURE

Controls framework

- Senior manager approval every 15 months
- Continuous monitoring
- Self-report
- Self-certification
- Whistleblower - reporting organization do it
- Spot check
- 3-/6-year audit cycle



Penalty structure

- Staggered penalty matrix based on risk and severity
- Federal penalty structure up to $1 million per day/per violation

Entities are required to utilize continuous monitoring of their reliability obligations and compliance programs in a manner that seeks out and identifies deficiencies. When identified, entities are required to immediately self-report any identified violations of the requirements through the use of self-report forms. The self-reported violation becomes a Possible Violation that is investigated by the NERC Regional Entity, and if a violation is confirmed, then the entity begins working with the enforcement department from the Regional Entity, which determines the penalty amount.

Entities subject to NERC regulation must also self-certify on a monthly, quarterly, or annual basis depending on the standard and the requirement. The self-certification establishes an auditable point in time when the entity is self-certifying a status on an individual requirement.

There is also a whistleblower capability, where anyone can contact NERC or a region and report a Possible Violation that will result in a Compliance Violation Investigation of the entity.

NERC also has a routinely scheduled 3-year or 6-year audit cycle that is utilized to assess an entity's compliance over the entire 3-year or 6-year period since the last audit. In addition, NERC has the capability to exercise a spot check on any standard or requirement at any time of any entity.

Through the Energy Policy Act of 2005, FERC has federal sanction capability that extends to NERC and the regions. Each standard has requirements that have been assigned risk and severity levels, and penalties will be determined using these assigned risk and severity levels. The sanction guidelines allow for penalties up to $1 million per day per violation.

REGULATORY EXAMPLE OF CYBERSECURITY POLICY

CIP-002: BES Cyber System Categorization — defining assets.

CIP-003: Security Management Controls

CIP-004: Personnel and Training

CIP-005: Electronic Security Perimeters (including interactive remote access)

CIP-006: Physical Security of BES Cyber Systems

CIP-007: System Security Management

CIP-008: Incident Reporting and Response Planning

CIP-009: Recovery Plans for BES Cyber Systems

CIP-010: Configuration Change Management and Vulnerability Assessments

CIP-011: Information Protection

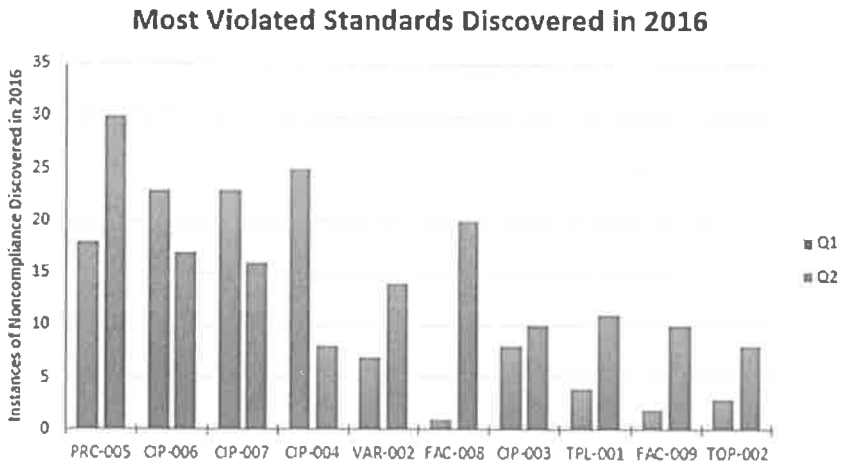
CIP-014: Physical Security of Stations

The NERC CIP-003 Standard addresses requirements around Security Management Controls with the requirements around cybersecurity policies that address the requirements of the CIP Standards. CIP-003-6 R1.1 lists the required cybersecurity policy topics that must be addressed for high- and medium-impact BES Cyber Systems. This can be separate individual policies or an overarching umbrella policy. The training requirements in CIP-004-6 R2.1 also require training on these policies.

Reference:
http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

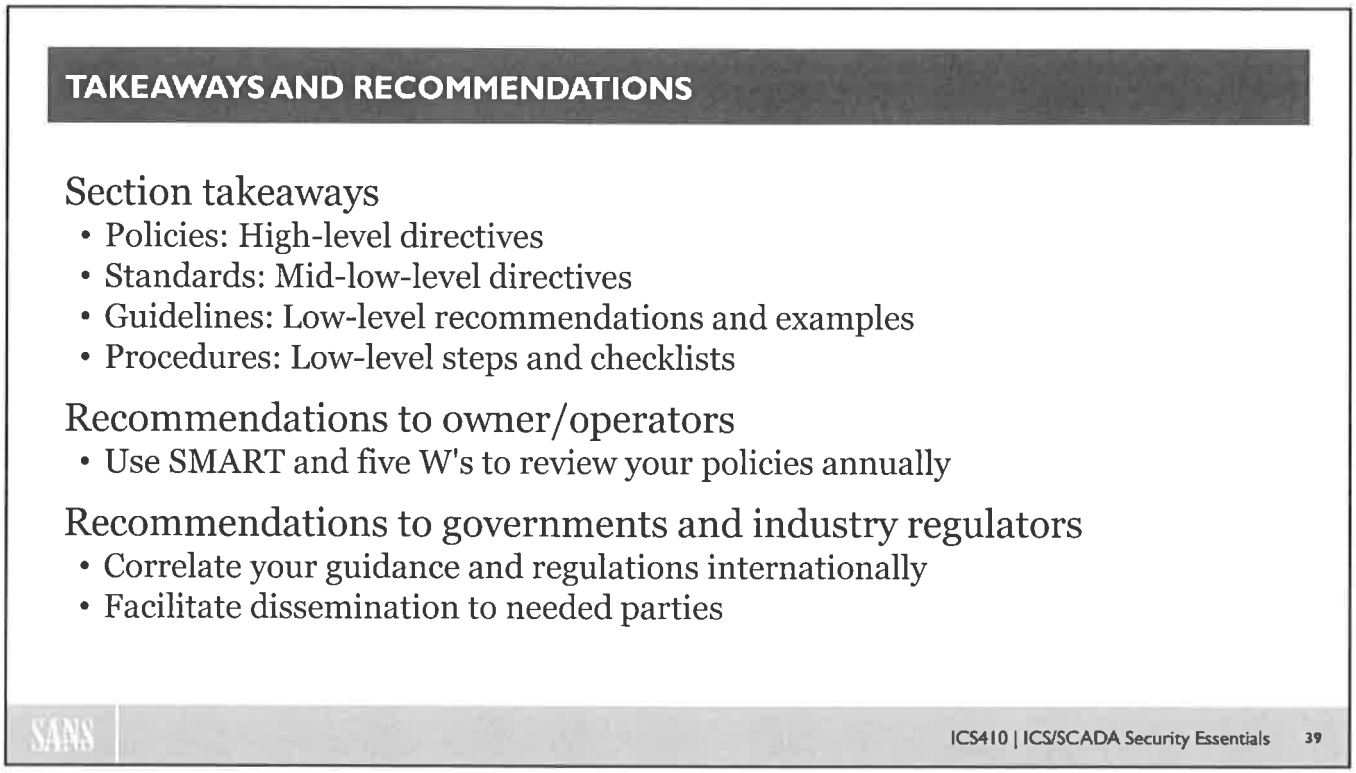
MOST VIOLATED NERC STANDARDS

CIP-003 is currently number 7 in the 10 most violated standards of 2016



NERC has more than 100 reliability standards, and it tracks the most violated standards of all time. The set of CIP Standards represents 10 of the 100-plus NERC Standards, and based on actual violations in Q1 and Q2 of 2016, the CIP Standards represent 4 of the top 10 most violated standards. The 10 CIP Standards have traditionally held 6–8 spots in the top 10 most violated standards of all time, which is an ongoing inventory of violations, a strong indication of the dynamic nature of the cybersecurity-focused standards versus the traditional reliability-focused standards, as well as the challenges of maintaining compliance with standards that represent repetitive reoccurring tasks that need to be performed on a large number of assets.

Reference:
http://www.nerc.com/pa/comp/CE/Pages/Compliance-Violation-Statistics.aspx



Policies, Standards, Guidelines, and Procedures
We learned the difference between a policy, standard, guideline, and procedure. *Policies* are the high-level documents that tie directly to corporate objectives. *Standards* are the documents with a set of requirements defining what must be done to support a policy. *Guidelines* are akin to best practices, giving methods and examples of how to meet the standards, and may change often. *Procedures* are step-by-step processes to perform actions that meet the requirements of the standards.

Writing a Policy
We also learned a great deal about the business drivers, roles, and various activities involved in creating a policy.

NERC CIP Example
Finally, we learned about an example policy written by the North American Electric Reliability Corporation (NERC).

Course Roadmap

Day 1: ICS Overview

Day 2: Field Devices and Controllers

Day 3: Supervisory Systems

Day 4: Workstations and Servers

Day 5: ICS Security Governance

1. Introduction
2. ICS Cybersecurity Programs
   - Starting the Process
   - Frameworks: ISA/IEC 62443, ISO/IEC 27001, NIST CSF
   - Using the NIST CSF
3. ICS Cybersecurity Policies
   - Policies, Standards, Guidance, and Procedures
   - Culture and Enforcement
   - Examples and Sources
4. Disaster Recovery
   - DR and BCP Programs
   - Modification for Cybersecurity Incidents
5. Measuring Cybersecurity Risk
   - Quantitative vs Qualitative
   - Traditional Models
   - Minimizing Subjectivity
6. Incident Response
   - Six Step Process
7. **Exercise 5.1: Incident Response Tabletop Exercise**
8. Final Thoughts and Next Steps
   - Other ICS Courses by SANS
   - Other SANS Curriculums and Courses
   - Netwars

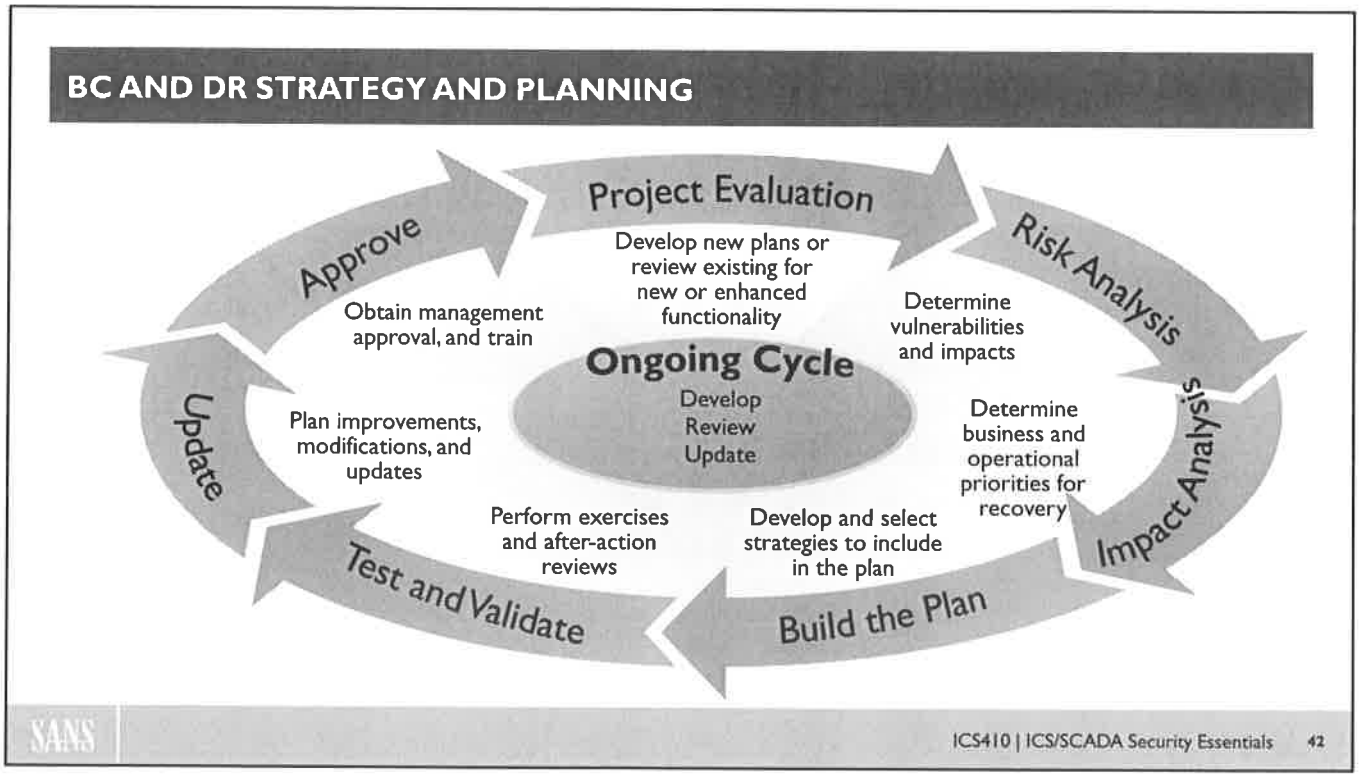
This page intentionally left blank.

Disaster Recovery

Applicable Standards:

- **NIST CSF v1.1:** RC.IM-1, RC.IM-2
- **ISA/IEC 62443-2-1:2009:** 4.4.3.4
- **ISO/IEC 27001:2013:** A.16.1.6, Clause 10
- **NIST SP 800-53 Rev. 4:** CP-2, IR-4, IR-8
- **COBIT 5:** APO12.06, BAI05.07, BAI07.08, DSS04.08

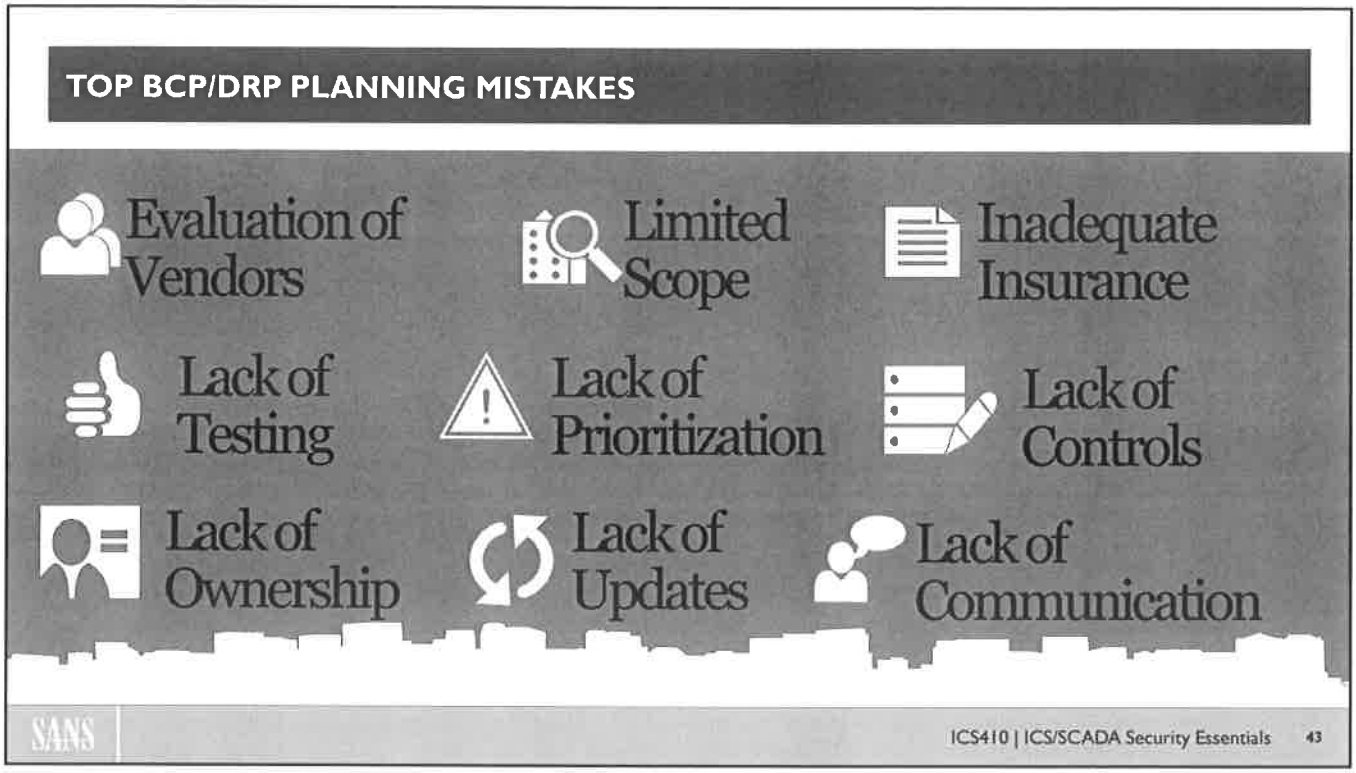
This page intentionally left blank.



This slide shows the basic steps that are necessary when developing a business continuity (BC) or disaster recovery (DR) plan. We start with Project Initiation, in which new or enhanced functionality is required. At this point, you must get management approval to start the project. Management is instrumental in making sure that you have access to the resources that are required to get the job done. The next sequence of steps in the process concern the company's vulnerabilities, their significance to the company, and what the company is going to do about them.

First, the company determines its vulnerabilities through a Risk Analysis. The company then assesses the impact that each of these vulnerabilities represents for the company by completing a business impact analysis. Realistically, no organization has the resources to deal with every vulnerability. Instead, in this step, the company prioritizes the vulnerabilities based on their likelihood and impact. Those vulnerabilities that represent greater risk to the company are identified so that steps to avoid their occurrence can be planned. In the event that those plans fail, the prioritized vulnerabilities can also be given priority in terms of recovery of affected operations.

Remember, not all losses are directly associated with the loss of money, although it will most likely affect the company financially in the long run. Do not forget to include the "intangible" losses, such as customer satisfaction or loss of consumer confidence. For instance, if a major e-commerce shopping site is down for a long time, consumers will become frustrated and will perhaps begin shopping somewhere else. At that point, it does not matter what caused the problem: Earthquake, flood in the data center, or a Denial-of-Service attack. The fact is that the site was down. The faster the company is able to recover, the better. Conversely, professional handling of a disaster can actually improve an organization's reputation with its customers and other stakeholders.



Top BCP/DRP Planning Mistakes
A number of other mistakes are commonly, almost predictably, made in contingency planning. These include the following:

Lack of BCP Testing / Over-Reliance on BCP
Many companies believe that just having a BCP (business continuity plan) is enough. The document is just a lifeless draft without adequate updating and testing. Organizations that test their BCP consistently find areas needing improvement and often critical flaws. The time to discover these is in advance of a real disruption. "Practice makes perfect." For less expensive testing, more frequently than your organization can afford full-fledged, off-site tests, try simulating a disaster, as in a business simulation game. Pretend something has happened, certain resources are no longer available, and have your personnel (who are assumed available) walk through the plan.

Too Limited in Scope
An incomplete BCP will not address all the organization's needs for recovery. The BCP needs to cover organizational processes and process dependencies, system recovery, as well as the replacement of key personnel if needed. The organization needs to continue to function throughout a disruption and beyond.

Lack of Prioritization
There is a need to prioritize the key business processes. The risk is to prioritize less-than-critical processes instead of the ones crucial for business survival. This is a time for thoughtful evaluation and decisions.

Lack of Plan Updates
The BCP should be updated periodically, especially when there are significant system, business process, or personnel changes.

Lack of Plan Ownership
Someone with the power to lead, influence, prioritize, and organize the BCP is instrumental to the success of the program. This is true during the planning and execution of the plan.

Lack of Communication
There is a need for clear and precise communication with all affected stakeholders of the organization, potentially: Employees, contract employees, vendors, business partners, customers, and shareholders. (This relates to public relations planning.)

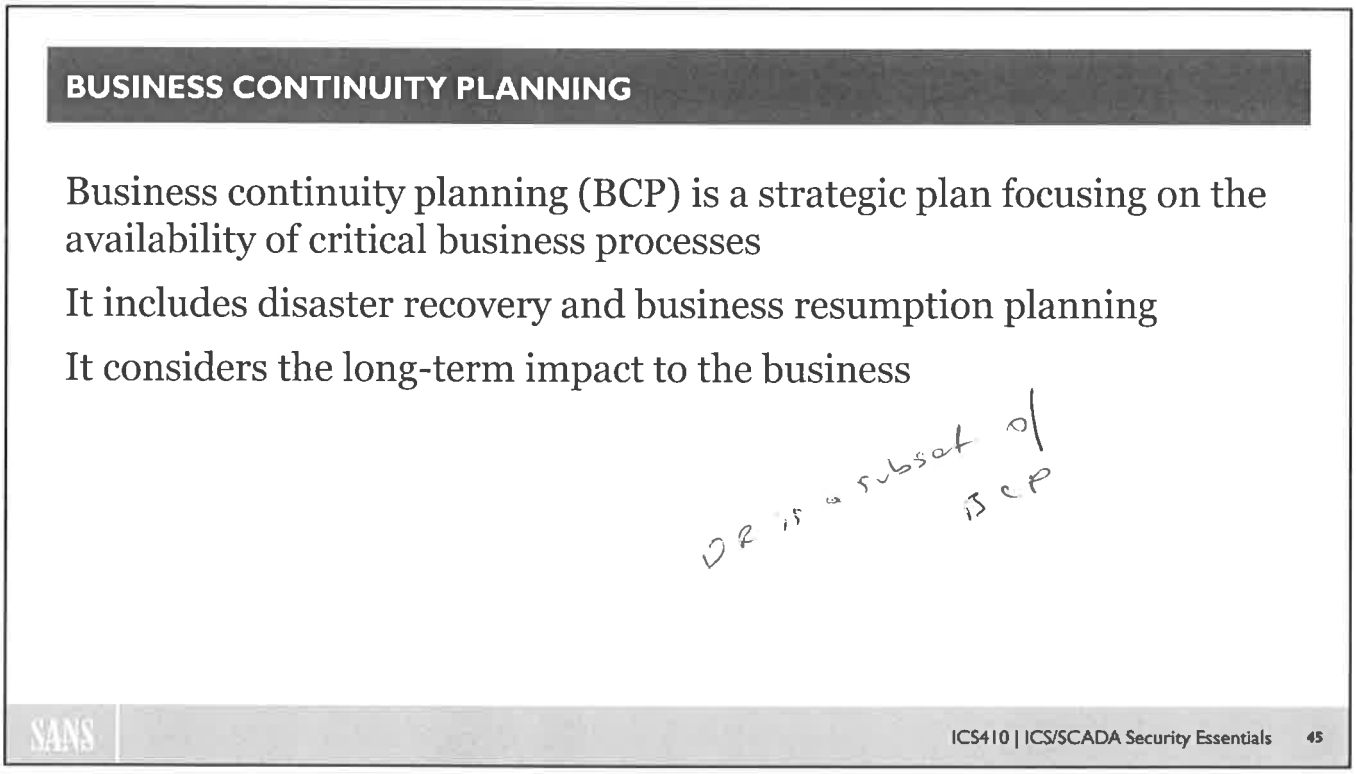
Lack of Public Relations Planning
Organizations often fail to consider public and investor relations, to limit the perceived disaster impact. This can literally make or break the organization. Years ago, tampering with the Tylenol pharmaceutical was leveraged by a strong internal PR at Tylenol that turned a disaster into a marketing opportunity.

Lack of Security Controls
During the recovery process, sometimes security controls are disregarded, resulting in a greater risk of exposure. Security controls likely may need to be altered and loosened during recovery. However, this should be a matter of conscious decision and empowerment that is built in to the plan. During execution of the plan, there should be strict adherence to the security controls incorporated into the plan.

Inadequate Evaluation of Vendor Suppliers
Many companies poorly evaluate recovery products (hot site, cold site, and planning software), relying on vendor-supplied information. This often leads to a solution that may not adequately address a company's needs.

Inadequate Insurance
Some organizations lack adequate insurance coverage and fail to support the filing of insurance claims, and these inadequacies result in delayed or reduced settlements. The plan may lack appropriate processes for capturing losses and recovery costs, without which the organization may realize a loss greater than otherwise necessary.

Summary
Use these examples of common mistakes as a checklist to review your organization's contingency planning – i.e., documentation, testing, integration with organizational processes and personnel, etc.



A business continuity plan (BCP) is defined as a plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation. Business continuity planning enables the quick and smooth restoration of business operations after a disaster or disruptive event.

The BCP is an overarching plan that details recovery from a disaster and business resumption planning, as well as a compilation or collection of other plans, including:

- Disaster recovery plan
- End-user recovery plan
- Contingency plan
- Emergency response plan
- Crisis management plan
- Other plans as required (for example, a server recovery plan or a phone system recovery plan)

A BCP is a business's last line of defense against risks that cannot be controlled or avoided by other risk management practices. In addition to an immediate action plan for recovering the business, the BCP should also consider a long-term plan that keeps the business running. For example, after the company has relocated resources and established operations in a new location, how should the business work to re-establish the disaster site? Long-term planning should also include public relations and possibly marketing, with a plan to maintain the positive, reliable image for the company following a disaster.

The BCP doesn't just define how a company should react to a disaster to keep the business operational; it must also define how the business will restore 100% of the operation, including the ability to continue to meet defined business goals.

These determinations are often defined in terms of:

- Recovery Time Objective (RTO)—how long a system can be unavailable while restoration occurs.
- Recovery Point Objective (RPO)—how current does the backup need to be that you are restoring from? Or how much data can you afford to lose? (Values that are developed for each critical system.)

The system analysis performed will identify the appropriate backup strategy, redundancy, backup site, and backup schedules.

Example of a BCP

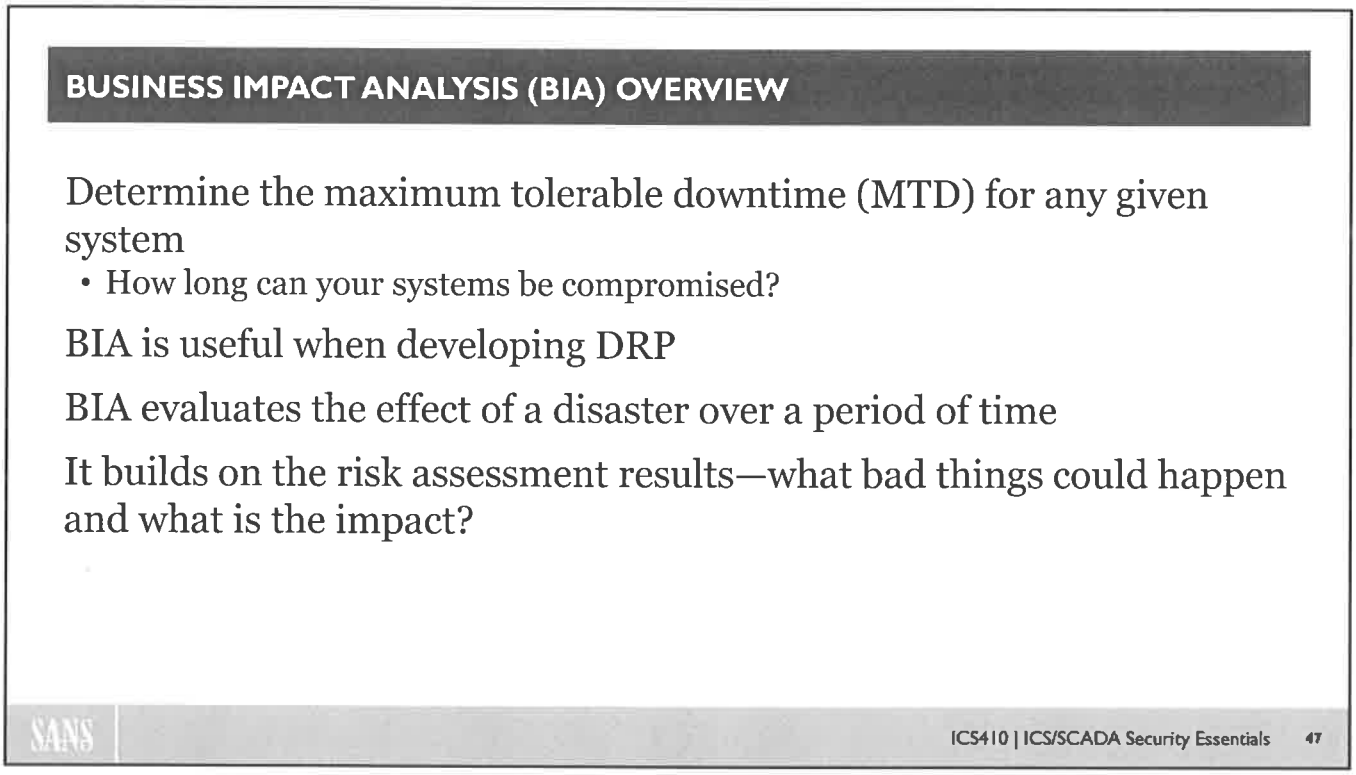
One organization, Morgan Stanley Dean Witter, was blessed with an individual who had the foresight to plan for the attack on the World Trade Center. Rick Rescorla was a unique individual. In 1985 and again in 1993, he identified the World Trade Center as a target for terrorist attacks. Rescorla is a prime example of what one person can do when committed to doing the right thing. Hundreds of people who were in those buildings on September 11 are alive today as a result of Rescorla's planning and because they practiced for such an attack.

Business Resumption Planning

Business resumption planning (BRP) is the generic term used to refer to the actionable plan that coordinates efforts to restore an organization to normal working order. This concept encompasses a wide scale of topics, from the immediate plans to restore business operations, to long-term business resiliency planning that will help an organization maintain a polished and undeterred image for consumers, even when faced with a disaster.

Summary

Like a business continuity plan, the BRP doesn't just involve IT; it involves all levels of the organization. The best BRPs that we've seen include how the organization will continue to meet and exceed the defined goals for a business following a disaster.



The business impact analysis (BIA) documents what impact a disruptive event might have on a corporation. The BIA prioritizes business functions versus risks to identify the criticality of functions and the time frame on which they must recover. Some business functions, if down for only a few seconds, might dramatically and detrimentally impact the business. Other business functions might be interrupted for days or weeks and have no negative effect on the corporation.

The primary goal of the BIA is to determine the maximum allowable downtime for any given system, or maximum tolerable downtime (MTD). Understanding the MTD for business processes is mandatory before designing your disaster recovery plan. Without the MTD calculation for systems, you won't know if the plan meets or exceeds the requirements of the business. While exceeding business requirements is usually a good thing, the cost of doing so may not be.

The process of developing the BIA typically involves interviewing the various key users of the various computer systems to get a better understanding of how a disaster could impact the ability to continue operations. Some of the key interview questions might include:

- What would be the impact of an information technology failure on cash flow and revenue generation?
- Would the disaster impact the level of service?
- How long could the outage last before it began to affect your productivity?
- Would there be irretrievable loss of data?
- What are the key resources that are required to be kept operating?
- At what point would those resources need to be in place?
- How does this process/system interact with other processes and systems? What are the dependencies on this process?

When putting together the BIA, the answers should come from, or be concurred by, executive management. At that level, management understands cost trade-offs such as between mitigation and loss, and has individual accountability either way. Lower management may err toward too much (that is, too expensive) risk avoidance, whereas upper management might prefer to accept certain risks and redirect mitigation resources elsewhere in the business. This is a common mistake in BCP/DRP planning.

REGULATORY EXAMPLE OF BCP / DR

NERC EOP-008-1 Loss of Control Center Functionality

- EOP (Emergency Preparedness and Operations)
- Ensure continued reliable operations of BES supervisory control

NERC CIP-009-6 Recovery Plans for BES Cyber Systems

- Ensure continued reliable operations of individual BES assets
- Establish business continuity and disaster recovery techniques and practices

The NERC EOP standards are a set of reliability standards that address emergency operations, and EOP-008 specifically addresses the requirements for entities to address the loss of control center functionality. NERC CIP-009 provides a set of requirements addressing recovery plans for Critical Cyber Assets.

Reference: http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

NERC EOP-008-1 LOSS OF CONTROL CENTER FUNCTIONALITY

Must provide for a backup control center

- Must be completely independent of the primary facility
- Must have necessary system tools and applications for operators
- Must provide adequate data and voice communications
- Must provide adequate power facilities, physical security, and cybersecurity
- Must address all communication and notification criteria

Must be able to execute transition in 2 hours or less

- Must have an operating process to keep both sites consistent
- Plan for actions to take during transition period

Must be reviewed and updated annually

Must be exercised annually

NERC EOP-008-1 requires applicable entities to provide for a location and method for performing backup functionality until the primary control center is restored. The backup control center must provide adequate power facilities for operations and provide physical and cybersecurity protections. The backup control center must provide for necessary operator tools, applications, and situational awareness, as well as all necessary voice and data communications.

These processes must operate in a manner that keeps both sites consistent and in many cases, requires real-time replication of data from site to site while in normal operations, so the backup site would be current in the event of an emergency condition. In addition, the transition period of personnel and systems being transferred cannot exceed 2 hours.

During the 2-hour transition period, the entities must plan for actions to take during the transition period, including communications and notification to necessary parties. These plans must be reviewed and exercised annually, and they must be performed in a manner in which they do not rely on voice or data communications from the primary control center.

Reference:
http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

NERC CIP-009-6 RECOVERY PLANS FOR BES CYBER SYSTEMS

Requires Recovery Plans to
- Contain procedures for recovering reliability functions performed
- Clearly identify roles and responsibilities
- Identify conditions for activation

Verification of backups
- Test sample recovery of data every 15 months
- Preservation of potential forensics evidence if possible

Test the recovery plans every 15 months
- Actual event
- Paper test
- Operational exercise
- For high impact BES Cyber Systems, operational exercise every 36 months
- Update plans with lessons learned in 90 days

Update plans with role changes or technology changes and communicate the updates within 60 days

While EOP-008-1 applies to certain entities depending on the functions they perform, CIP-009-6 applies to certain identified BES Cyber Systems within an organization depending on the impact they have on BES. Depending on the entity, they may be subject to EOP-008 and not CIP-009, or reverse, or neither, or both.

CIP-009-6 requires the recovery plans to address the following: Conditions for activation of the recovery plan(s), roles and responsibilities of responders, processes for the backup/storage of information required to recover BES Cyber System functionality, and processes to verify the successful completion of the backup processes. In addition, the plans need to address retention of potential cybersecurity incident related information if possible.

Testing and updating the recovery plans is required every 15 months, and the test can be performed through recovery after an actual event, or through a paper test as you evaluate procedures, contact info, and system restoration or failover procedures contained in the recovery plan, or you can perform an operational exercise. For certain systems, an operational exercise must be performed every 36 months.

After completion of these tests, lessons learned follow-ups must be documented and updated as well any updating the plans based on organizational role or responsibility changes or technology changes.

Reference:
http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

TAKEAWAYS AND RECOMMENDATIONS

Section takeaways

- ICS Cybersecurity Teams often don't own BCP and DR
  - Often already created for each critical ICS process
  - But we can influence them
- Most plans fail to consider or properly respond to cyber events

Recommendations to owner/operators

- Modify plans to include proper cybersecurity incident responses

Recommendations to vendors

- Create or improve your cybersecurity emergency response services for customers
- Educate customers in appropriate cybersecurity responses for your products

This page intentionally left blank.

Course Roadmap

Day 1: ICS Overview

Day 2: Field Devices and Controllers

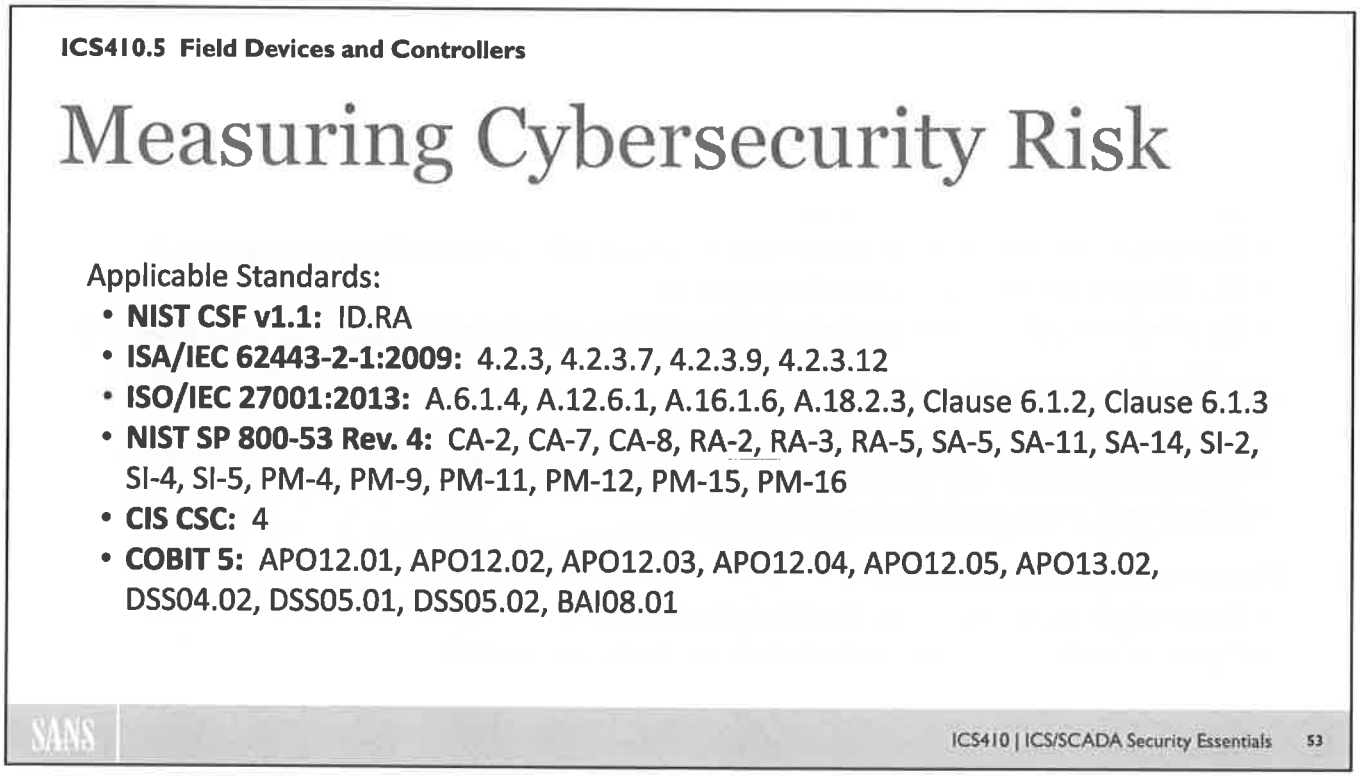
Day 3: Supervisory Systems

Day 4: Workstations and Servers

Day 5: ICS Security Governance

1. Introduction
2. ICS Cybersecurity Programs
   - Starting the Process
   - Frameworks: ISA/IEC 62443, ISO/IEC 27001, NIST CSF
   - Using the NIST CSF
3. ICS Cybersecurity Policies
   - Policies, Standards, Guidance, and Procedures
   - Culture and Enforcement
   - Examples and Sources
4. Disaster Recovery
   - DR and BCP Programs
   - Modification for Cybersecurity Incidents
5. Measuring Cybersecurity Risk
   - Quantitative vs Qualitative
   - Traditional Models
   - Minimizing Subjectivity
6. Incident Response
   - Six Step Process
7. **Exercise 5.1: Incident Response Tabletop Exercise**
8. Final Thoughts and Next Steps
   - Other ICS Courses by SANS
   - Other SANS Curriculums and Courses
   - Netwars

This page intentionally left blank.



This page intentionally left blank.

RISK APPROACHES

Quantitative Risk Assessment

- Preferred for business decision since it is usually in monetary amounts
- Is risk greater than cost to address risk?
- In cybersecurity, these are often speculative values unless directly tied to assets

Qualitative Risk Assessment

- Needed for most cybersecurity risk assessments
- Results typically categorized as low, medium, or high
- Could use 1–10 point scales like CVSS

Fewer categories means

- Less subjectivity and less likelihood of error
- Greater difficulty at prioritization and decision-making

There are two risk assessment approaches: Qualitative and quantitative. In quantitative risk assessment, we try to assign an objective numeric value; typically, this value represents a monetary loss value. Qualitative risk assessment, however, deals with more intangible values and focuses on variables and not just the monetary losses.

Quantitative risk assessment is a far more valuable business tool because it works on metrics; usually in dollars. The bottom-line cost in dollars is what management is looking for when trying to understand the implications of how a risk can affect the organization.

Qualitative risk assessment is much easier to perform and can identify high-risk areas. For instance, you need to perform a risk assessment to determine the impact of installing a wireless LAN access point in your organization. The first order of business is to determine the vulnerabilities, threats, and therefore the risks of using a wireless LAN. Then you determine if those risks apply to your organization and determine the likelihood that you are at risk. One of the risks of using a wireless LAN is the possibility of someone sniffing the wireless network traffic, and that a misconfigured access point can allow rogue client connections. These are real risks that need to be addressed. Can you put a monetary value on these risks? If someone does connect to your network via the open access point, how much is that going to cost your company in lost revenue?

As you can see from this example, quantitative risk analysis in this situation does not quite work. A qualitative approach is much better because we can arrive at a less subjective result. In qualitative risk assessment, the results are typically categorized as low-, medium-, or high-risk events. A person operating a wireless LAN access point in the house in the country, where the nearest neighbor is 5 miles away, is at a low risk of having someone trying to connect to the network. A company in the middle of a high-tech park, with an access point that allows rogue connections, has a high risk.

RISK ASSESSMENT METHODOLOGY

Easier-to-answer questions

- What can be compromised? (Asset/Process)
- What or who could compromise it? (Threat Actor)
- What could the threat actor do? (Threat)
- What weakness can the attacker exploit? (Vulnerability)
- What could this mean for the company? (Risk)
- If it happened, how bad could it be? (Impact of Risk)

Harder-to-answer questions

- How likely is it to occur? (Likelihood)
- How often could it happen? (Frequency)

How reliable are the answers? (Subjectivity)

To decide between accepting, mitigating, or transferring the risk, we need to better understand the risk and how it affects us.

When evaluating risk, it is helpful to ask yourself some key questions listed in the slide above.

The answers to these questions help us focus on the actual threats and gain a better understanding of their impact if they were to actually happen. The first question is to ask ourselves: What exactly are we afraid of? What is the actual threat? Is the threat something tangible? Can we accurately define the threat?

And if we can define the threat, what damage could it cause? What is the probable extent of the damage? For instance, the damage could be anything from a few corrupted files to a complete destruction of our critical processes, causing loss of life and damage to the environment. In other words, what is the impact of the risk? Another variable to consider is the frequency of the threat. How often could this threat happen? Is it just once or can it occur more often?

The last question relates to the recognition of uncertainty. That is, how sure are you of the answers to the previous questions? Can you validate and prove your answers? This might be a difficult question to answer because it might be hard to accurately perform our risk calculations on operating systems or new programs when new vulnerabilities are constantly being discovered.

CALCULATING RISK

Traditional risk calculations

- Single Loss Expectancy (SLE) = Asset Value × Percentage of Loss (EF)
- Annualized Rate Occurrence (ARO) = Likelihood × Frequency
- Annualized Loss Expectancy (ALE) = SLE × ARO

Frequency and likelihood are near impossible to predict for cybersecurity

What if you can't even tie an event or defense to an asset?

For ICS guidance, we can look at FERC Order 706

- "Because there is insufficient data available to determine frequency, it should be assumed that an event will occur."
- "Risk-based assessment methodology should focus on the consequences of an outage, not the likelihood of an outage."

When all is said and done, in the end, it all comes down to money. What management will be considering is, "How much financial loss are we willing to accept in a single (threat) event?" If a company's database is compromised and that database contains your proprietary (and valuable) secret formula for your next revolutionary drug, then you could not afford even one risk to your system that might lead to the theft of this formula. Remember, we stated that risk involves uncertainty. The uncertainty here is that we cannot accurately determine the exact value of the formula (it might make millions of dollars, or it might not make any money at all because the formula might not work).

What this leads to is the calculation of the Single Loss Expectancy or SLE. The SLE is the dollar value that is assigned to a single event. That is, it is the organization's loss from a single event. The Exposure Factor (EF) is the percentage of loss a threat event would have on the asset. The EF is expressed in terms of 0 to 100% loss of an asset. What happens when the event occurs more than once? We then calculate the Annualized Loss Expectancy or ALE. The ALE is the annual expected financial loss from a threat.

both replacing the asset and cleaning the mess

EXAMPLE: NERC CIP'S CONSEQUENCE-DRIVEN RISK PRIORITIZATION

ICS systems and components can be characterized by their intended function
- From safety systems to auxiliary services
- Measure in 6 levels (see notes for Level breakdown)

Determine risk by itself to categorize assets into levels
- The most trusted/protected, are Level 0 systems, the least are Level 5
- Changes in trust require security enforcement to each level's trust boundaries
- Can be used to establish use policies and settings or controls (e.g. types of wireless allowed)

Use likelihood and frequency to help prioritize actions inside each level

ICS applications are best prioritized by the function a specific system provides as measured against the consequences involved if the system did not function properly or were misused.

Functions, for our purpose of prioritizing, can be described as the following (you might add levels or expand definitions for local use):

Level 0 – Safety and Emergency Action and Shutdown
Level 1 – Control (closed loop regulation or protection systems in the power system)
Level 2 – Supervisory Control
Level 3 – Monitoring and Alarming
Level 4 – Telemetry only
Level 5 – Auxiliary services

These functions can be mapped to consequences that may occur if the function is disrupted, affected, or misused. To identify specific consequences, an analysis effort including process engineers can be performed to identify how the specific process or equipment/machinery could be affected if the function were lost or misused. These efforts can be modeled off existing risk assessment methods used in engineering, such as PHAs, Hazops, LOPA, and FSAs. Having a security analyst involved makes sure the team performing the analysis does not develop blind spots around what is possible or attacks that could impact a specific system design. Some systems can be prioritized as "mission-critical" as they are necessary to the proper function for the plant or process to run. Mission-critical systems may not always be apparent as some of the requirements can be overlays such as regulation. In these cases, the plant could physically operate safely, but the loss of the system might trigger a regulatory threshold that requires shutting down that plant (for example, emission-monitoring sensor reporting on the stacks of a coal plant).

Trust is an important security concept and it can be defined in gradients from most trusted to least trusted. Changes in trust gradient would require security enforcement and controls to interconnect and transverse trust boundaries. This is a material concept that forms the basis for ISA-99/IEC-62443 architectures. Keep in mind that systems used to set or store configurations should be placed into the correct level if they can connect with those devices (for example, an engineering workstation that can interface with a safety system would be considered Level 0).

Examples of systems that may be included in the different levels:

Level 0 – Safety and Emergency Action and Shutdown

Safety Instrumented Systems (SIS), Emergency Shutdown Systems (ESD), Safety System, Safety Logic Solver, Fire and Gas (F&G), safety connected instruments, Safety Controller, any device with a Safety Instrumented Function (SIF), Health and Safety systems (e.g. radiological monitoring systems), etc.

Caution: Some ICS systems have merged safety functions and control. These integrated control and safety systems or functions should be treated as Level 0 (the highest trust) systems.

Level 1 – Control

Process controllers, power system protection (relays), process shutdown (PSD), Programmable Logic Controllers (PLCs), remote terminal unit (RTU), control servers, etc.

Level 2 – Supervisory Control

Primary HMIs, alarms required for operator control actions, etc.

Level 3 – Monitoring and Alarming

Alarm servers, sequence of event recorders, local historians, HMIs, etc.

Level 4 – Telemetry only

Metering systems, historians, telemetry collection systems, etc.

Level 5 – Auxiliary services

Weather systems, messaging system, work ticketing system, scheduling system, maintenance systems, CCTV systems, laboratory systems (can be connected to Level 1 systems), corrosion monitoring systems, emission monitoring systems, etc.

Caution: You might identify other "mission-critical" systems that could fall in Level 2 as their loss would require a controlled shutdown of the plant or process. You may also characterize your security systems or those controls that help maintain the integrity of your Level 0 systems as being on par or in the same trust gradient. Many organizations use security services, applications, and devices to protect high trust systems, but they don't apply the same level of security. This is common when security services are provided from the general enterprise network. The best rule of thumb is to have all your security devices managed from a similar level or higher level of trust/protection than the system that you are protecting.

RISK ACCEPTANCE AND COST-BENEFIT ANALYSIS

Who in your organization decides level of risk to accept?

Usually compare the cost of countermeasures with the value of reduced risk

- Cost includes implementation, maintenance, and monitoring
- Easy countermeasures generally show cost benefit
- Hard effective countermeasures also should show cost benefit

Organizations often provide insufficient staffing for new security solutions

- General rule of thumb: Minimum of 1.5 FTEs per new solution
- Full Time Equivalent (FTE)

→ prior to merge systems

Biggest benefits to the organization are countermeasures that protect the revenue flow

An important question you will need to answer is, "Who in your organization is actually authorized to decide what level of risk the organization will accept?" An issue that comes up from time to time is that lower-level managers make risk decisions that can potentially adversely affect the entire organization. This is partly a function of not understanding the technologies and risks involved. One method of mitigating this is with awareness training.

Another consideration factor is the cost of the safeguard versus the actual value of the asset. It makes sense that the cost of the protection should not be more than what the asset is worth. Would you buy a $5,000 safe to protect a ring that is worth only $100?

Cost-benefit analysis is the comparison of the cost of implementing countermeasures with the value of the reduced risk. Can you accurately determine if the countermeasure is 100% effective? Antivirus software is known to fail against unknown viruses, especially if the virus signatures are not up to date. Companies with firewalls are not 100% protected because firewalls can be compromised (or bypassed) and because traffic containing attacks may legitimately pass through the firewall.

Benefits are the reduction in the risks your company is exposed to. Keep in mind that the biggest benefits to the organization may be the countermeasures that protect the revenue flow. This is especially true if your organization is involved in ICS. The cost of a countermeasure is more than just the initial cost. There is the labor cost of monitoring the devices and the life-cycle cost.

REGULATORY EXAMPLE OF RISK-BASED ASSESSMENT

CIP-002-5.1 BES Cyber System Categorization

- Identification and categorization of cyber systems and assets
- Review the list of identified systems and assets every 15 months
- Senior manager review and approval every 15 months

This is a shift from prior regulation

- Asset owners previously identified what was critical
- Now a criteria-based list is provided

CIP-002 is sometimes referred to as the scoping standard in that the Attachment 1 criteria is used to identify the assets and BES (Bulk Electric System) Cyber Systems in scope for applicability to the requirements. The requirements apply based on the criteria of high, medium, or low and the applicability of each requirement part.

Organizations subject to the NERC CIP Standards must consider the following asset types when evaluating the criteria of Attachment 1:

i. Control Centers and backup Control Centers
ii. Transmission stations and substations
iii. Generation resources
iv. Systems and facilities critical to system restoration, including Blackstart Resources and Cranking Paths and initial switching requirements
v. Special Protection Systems that support the reliable operation of the Bulk Electric System
vi. For Distribution Providers, Protection Systems specified in Applicability section 4.2.1 above

Reference:
http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

TAKEAWAYS AND RECOMMENDATIONS

Section takeaways

- Calculating risk is hard and always subjective
- Minimize subjectivity by minimizing subjective inputs

Recommendations to owner/operators

- Make decisions first based on risk alone for initial categories
- Prioritize inside each category based on likelihood and frequency

Recommendations to governments and regulatory bodies

- Follow DOE's recommendation of risk first
- Minimize regulatees' ability to use highly subjective inputs to avoid remediating high-risk vulnerabilities

This page intentionally left blank.

Course Roadmap

Day 1: ICS Overview

Day 2: Field Devices and Controllers

Day 3: Supervisory Systems

Day 4: Workstations and Servers

Day 5: ICS Security Governance

1. Introduction
2. ICS Cybersecurity Programs
   - Starting the Process
   - Frameworks: ISA/IEC 62443, ISO/IEC 27001, NIST CSF
   - Using the NIST CSF
3. ICS Cybersecurity Policies
   - Policies, Standards, Guidance, and Procedures
   - Culture and Enforcement
   - Examples and Sources
4. Disaster Recovery
   - DR and BCP Programs
   - Modification for Cybersecurity Incidents
5. Measuring Cybersecurity Risk
   - Quantitative vs Qualitative
   - Traditional Models
   - Minimizing Subjectivity
6. Incident Response
   - Six Step Process
7. **Exercise 5.1: Incident Response Tabletop Exercise**
8. Final Thoughts and Next Steps
   - Other ICS Courses by SANS
   - Other SANS Curriculums and Courses
   - Netwars

This page intentionally left blank.

Incident Response

Applicable Standards:

- **NIST CSF v1.1:** RS
- **ISA/IEC 62443-2-1:2009:** 4.3.4.5.1
- **ISO/IEC 27001:2013:** A.16.1.5
- **NIST SP 800-53 Rev. 4:** CP-2, CP-10, IR-4, IR-8
- **CIS CSC:** 19
- **COBIT 5:** APO12.06, BAI01.10

This page intentionally left blank.

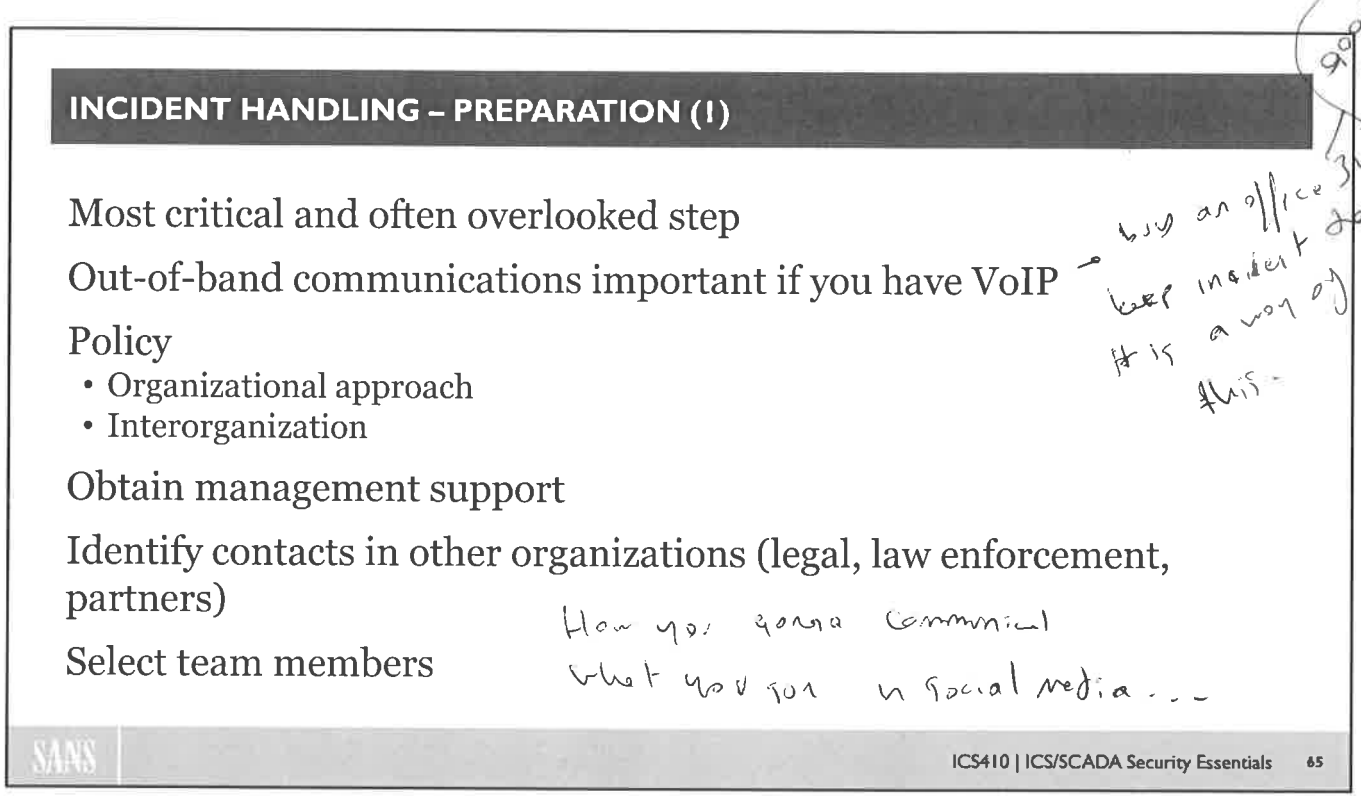
detection is a must.
response is a must.
detection without response is useless.

INCIDENT HANDLING PROCESS

Preparation
Identification
Containment
Eradication
Recovery
Lessons Learned

Based on the importance of incident response across the industry, it is important that a clear and standard process be followed. To create a starting point, the US Department of Energy (DOE) led an initiative to build a six-step process back in the early 1990s. The six-step process used in this course and throughout the industry is based on the original process developed as part of a joint effort led by DOE.

The six steps listed here can help serve as a road map or a compass, if you will, to develop a phased approach to incident handling. Keep in mind that for this process to be successful, each step must be followed.



The preparation step is the first and most critical step of the incident handling process. The tasks associated with this step must be performed in advance, before the incident has occurred. This is the reason why it is often overlooked, or even skipped. SANS recommends that you spend enough time preparing all the elements that are required during an incident, with the goal of increasing the efficiency and success of your incident handling efforts.

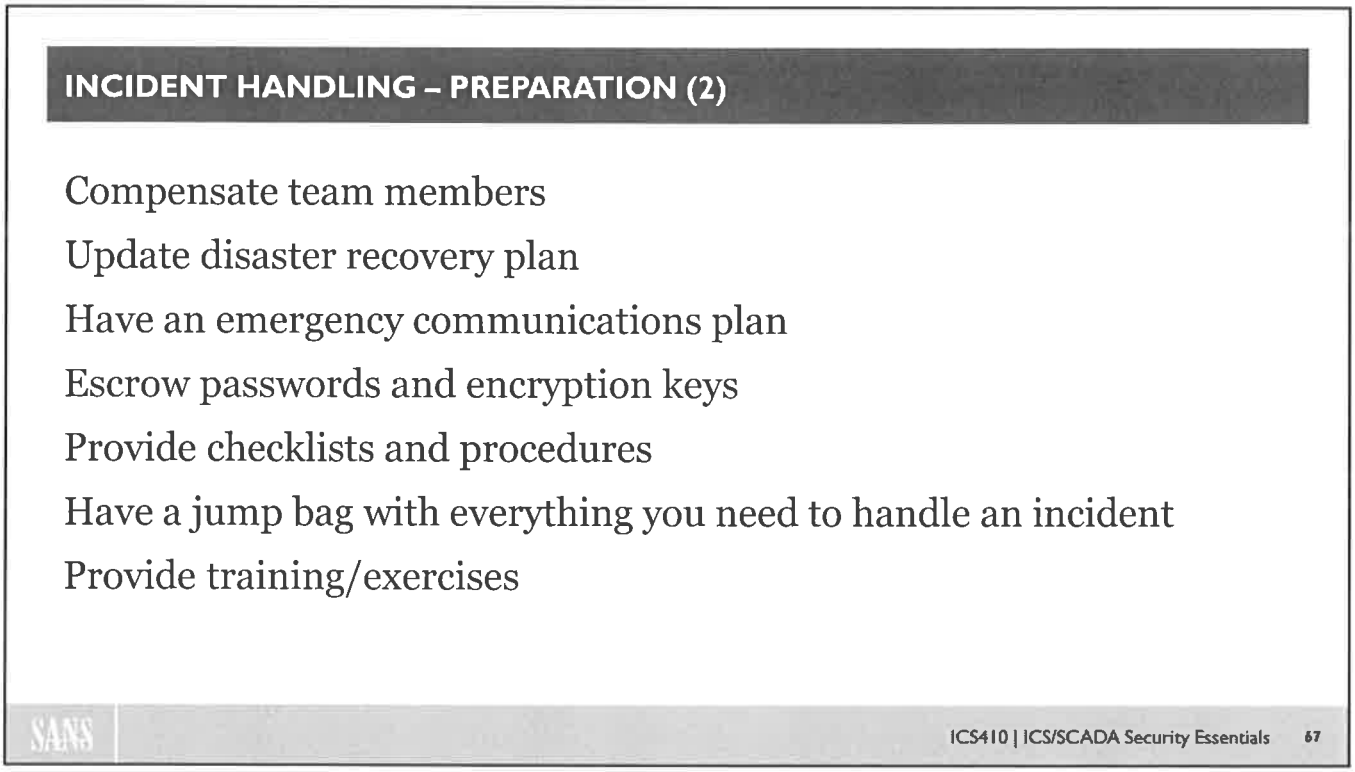
When it comes to incident handling, planning is everything, and preparation plays a vital role. It is important to have a policy in place that covers an organization's approach to dealing with an incident. One item that a security policy needs to cover is whether a company is going to notify law enforcement officials or remain silent when an incident occurs. The answer to that may depend on the severity of the incident; if so, what guidelines should the responder use to decide whether to call? If you are going to contact law enforcement, have a list of phone numbers for each agency you may need to involve.

Another important item to consider is whether to contain the incident and move into cleanup phases or to observe the attack in an attempt to gather more evidence. The policy should also contain direction for interorganization incidents and how the company works with other companies regarding an incident.

Incident handlers can be under extreme pressure. Consider a worm that infects your entire infrastructure, effectively making your network systems unusable. This is one reason incident handling teams must never rely on Voice over IP. If you have a VoIP installation, consider the use of cell phones, walkie-talkies, or some other backup method of communications. Incident handling can become a large-scale effort involving many people on many systems simultaneously. This should be taken into account during the planning phase.

The time to make these types of decisions is before the incident, keeping senior management and legal staff apprised of any changes to policy. Because of the sensitive nature of incident handling, any decisions made could greatly affect your career down the road if you did not get approval or reach consensus with management. The last thing you or your company wants is for senior management to question or doubt the decisions that were made during an incident.

When selecting members of the team, keep in mind that not everyone makes a good incident handler. There are some smart people in this industry whose personalities do not lend themselves to work under immense pressure and as part of a team. People who like to work solo and need to be the hero usually do not make good team members. Ideally, a person should have a strong technical background, thrive in a team environment, and have the ability to make sound decisions grounded in reality.



As the incident response team begins to mature and has responded to several large incidents, it is possible that members of the team will get burned out and leave the team. Although this is certainly understandable, an approach you may want to take is to provide compensation and other rewards for members of the team. This may run counter to your current policies, but keep in mind that incident handlers are often called to perform their duties after normal business hours, weekends, and holidays while under a lot of pressure to get things restored as quickly as possible.

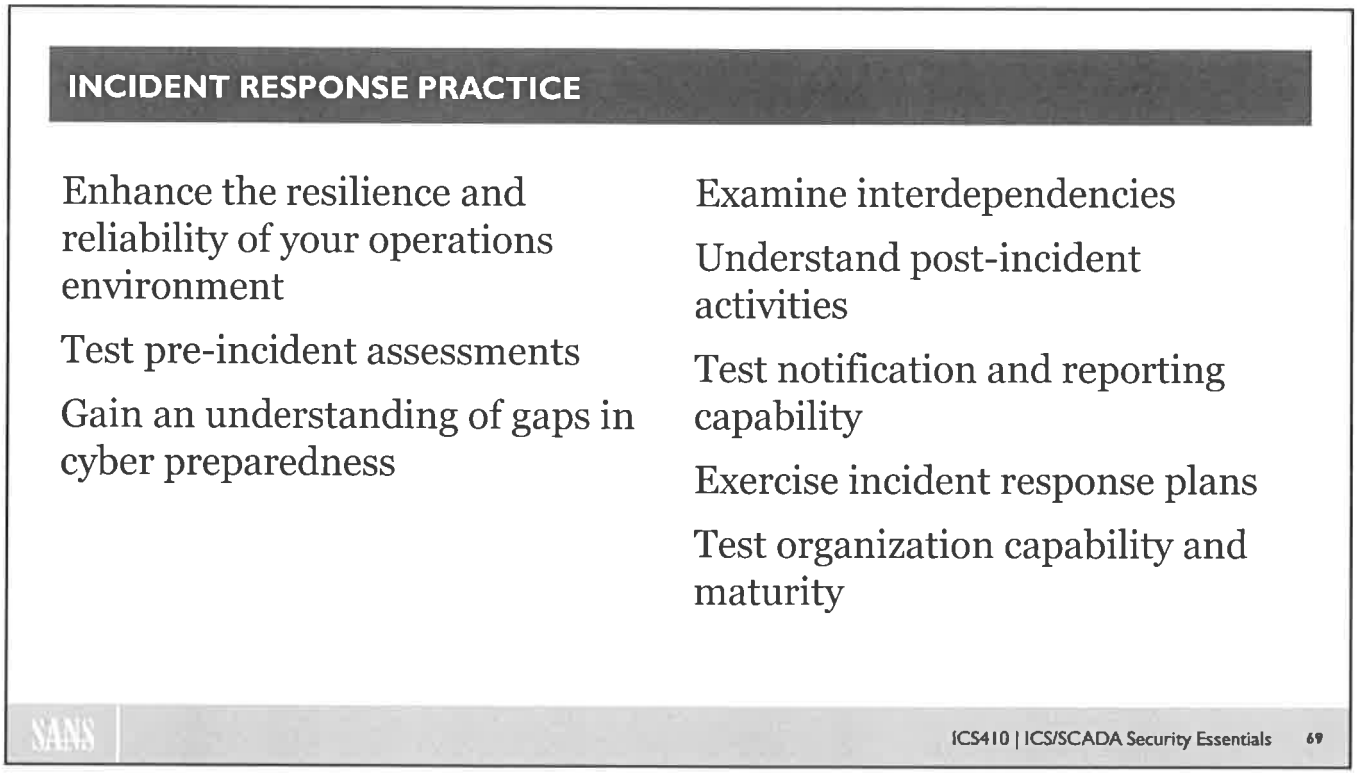
During the preparation phase, an organization should make plans to update its disaster recovery plan to include incident handling. After all, what is a disaster? It is an incident and needs to be handled as such. Although disaster recovery plans are often thought of as a checklist to get a business back up and running as quickly as possible, the skills possessed by the incident handling team could be put to good use to reach this goal. In addition, the disaster recovery plan and the incident handling procedures guide should contain information for emergency communications.

The issue of making privileged passwords available to others can be a delicate situation. However, in an emergency, a handler may need access to critical systems.

One idea to consider is to incorporate a procedure where system passwords are kept in sealed envelopes in a locked container or data center until they need to be used. This may seem cumbersome, but it does work and keeps the passwords private until they are needed by the incident handling team. For this to work, the system administrators must ensure to keep the passwords in the sealed envelopes up to date, and the incident handlers must make every effort to tread lightly on the systems, inform the system administrators of any changes made, and above all, never use a privileged password unless they are qualified on that operating system. One thing that will certainly make an incident worse is having someone who has no idea what he is doing issuing commands as administrator or root.

Our computing environments are complex and will change over time. Training is critical for each member of the incident handling team. Memory fades over time, especially if the members are not working on honing their skills on a regular basis. Having a checklist on how to bring a system down safely or on how to restore a system from tape can help in preventing errors and can reduce the stress on the handler. If your team is following a checklist and the resulting operation fails, it may be the fault of using an outdated checklist on a regular basis, so ensure they are updated to your organization's current environment.

Reaction time to an incident is absolutely critical. Every effort should be made to find members of the incident handling team who will be able to respond on short notice. For example, an incident handler who has a 2-hour commute into work may not be that helpful in a situation that requires immediate attention. One way to mitigate the effects of delayed reaction is using what the military calls a jump bag. This bag would contain in a central location everything needed to respond to an incident. Items such as contact numbers, checklists, telephone, notepad, and pencils are items that you would want to include. Also, as far-fetched as it sounds, spare network cables, a hard drive, a mini-hub, and tools for working on a PC should be considered essential.



If the first time you dust off your incident response plan (IRP) or communication and notification plan is when you have an incident, then it is unlikely that you will handle the incident in an appropriate manner. Much like an athlete, practice is critical if you expect to increase your performance and overall ability.

Performing exercises will help improve the abilities of your players to more quickly identify events of interest, provide necessary training on what players should do, and almost equally important, what they should not do.

Many organizations have a mature risk assessment process that has been leveraged to examine the risk of impact to an operating environment. Mature risk assessments involve internal business units responsible for an operational environment, as well as across business units that interface or support the operational environment. As you build advanced scenarios that simulate impacts to components of your operating environment, you will further examine the pre-incident risk assessment determinations.

As players work through their response plans and attempt to contain, eradicate, and recover assets, it may become apparent that additional layers of protection or capabilities would improve overall capabilities.

Players and planners will likely identify important interdependencies across business units and internal or external partners that may have not previously been identified as potential stakeholders in your incident response process.

Cross-Business Unit collaboration, reporting, and incident assessment (including escalation procedures) include broad business coordination (C-suite, public affairs, IT, operations, legal, corporate communications, customers, risk committee, compliance, regulatory agencies, vendors, supply chain, facilities, physical security, law enforcement, and more).

Many incident response plans fail to identify a true process of incident de-escalation or Cross-BU prioritization and resource allocation. There may also be important reporting requirements post incident including:

- Regulatory reporting
- Financial impact reporting

- Lessons learned documentation
- Root cause analysis
- Document best practice items identified for broader implementation

Many organizations are required by regulation to perform routine communication tests and test reporting and notification capabilities. For organizations that do not have external requirements, it should still be pursued in a test or practice opportunity rather than discovering that you do not have a means of communication during an incident, either due to poor documentation or due to primary communication system loss.

Many organizations' incident response plans do not provide adequate guidance and appropriate procedures; further, many employees may not even be aware that an IRP exists or where it is. During an incident, it would be difficult to ensure appropriate actions are taken if a playbook is not well understood and practiced.

Exercises not only provide the ability to examine the resiliency and capability of your systems and your defenses, but they also provide the ability to examine your personnel capabilities and maturity in responding to an attack. The greatest systems and plans are unlikely to succeed without skilled, knowledgeable, and capable staff.

all incidents start with a minor incident. So anyone should identify incidents and communicate to response team

INCIDENT HANDLING – IDENTIFICATION (1)

Who should identify an incident?

How do you identify an incident?

- IDS alerts, failed or unexplained event, system reboots, poor performance...

Be willing to alert early, but do not jump to a conclusion

- Look at all the facts
- Accurate reporting

first examine, if needed, escalate.

Notify correct people

Utilize help desk to track trouble tickets to track the problem

426 days: Average time from compromise to detection

When it comes to identifying an incident, members of the team should stay in their realm of expertise. You would not want a Windows expert digging around a UNIX system, and vice versa.

Some possible signs of an incident that may warrant further investigation essentially include anything suspicious, such as intrusion detection alerts, unexplained entries in a log file, failed logon events, unexplained events (such as new accounts), system reboots, and poor system performance.

Being able to correctly identify an incident could be the difference between cleaning up the problem in a few minutes and causing your organization's network to be down for several hours or even days. Obviously, any system outage could potentially cost your company a lot of money, so it is important to identify an incident correctly the first time and respond accordingly. For example, after a fire alarm is pulled and a building evacuated, qualified firefighters respond to the scene and investigate. Only then does the firefighter in charge at the scene authorize re-entry into the building. This should be the paradigm we work under; be willing to alert early, have trained people look at the situation, and be able to stand down quickly at a minimum of expense if nothing is wrong. No matter which course of action you decide to pursue, make certain you have mechanisms in place to correctly identify an incident.

There is nothing wrong with alerting early if you maintain situational awareness, and everyone understands this might not be an actual incident. All attempts should be made to avoid overreacting to the situation and escalating it too fast, only to realize an hour later that you made a mistake. If that happens enough times, you could fall victim to the "boy who cried wolf" syndrome; and then when a real incident occurs, no one will believe you because of the false alarms.

Chances are your organization has a 24/7 help desk operation that would be ideal for helping out with tracking the incident and maintaining a paper trail. They could also be utilized to facilitate communication and contact other personnel as the situation warrants.

According to Verizon's *2013 Data Breach Investigations Report* (DBIR), the average time between a compromise and detection of said compromise is 426 days.

INCIDENT HANDLING – IDENTIFICATION (2)

Assign a primary handler

Do not modify information Collect the info. regularly. Then compare what is now.

Identify possible witnesses and evidence

Determine whether an event is an incident events are potential incidents

Identify evidence

It is important to keep in mind that a primary handler should be assigned as a team leader to keep the process flowing while also making sure that no steps are overlooked or missed. For smaller incidents, often of the "Would you check this out?" category, there isn't a need to send a core team of incident handlers. It is a recommended practice to have a core team of well-trained handlers and also have incident handling skills and training as part of the job description for security officers and system administrators. An organization that adopts this approach benefits by having multiple layers of "firefighters."

However, in such a case, it is important to assign tasks in a way that encourages cooperation among the team and allows them all to succeed. When assigning tasks to part-time members of the team, do so in a way that it is clear what is expected of them: The quality of their investigation, their responsibility to preserve and collect evidence, what documentation they should produce, and when it is due. It is also important that they know who they should contact if they feel they need additional guidance or support.

After you determine that the event is actually an incident, the handler may decide to take the steps needed to build a criminal or civil case. In this situation, witnesses should be identified, and a written statement of what they heard or saw should be taken immediately while the information is still fresh in their minds. If a decision is made to involve law enforcement, make sure senior management is notified, unless you have a detailed policy to follow.

INCIDENT HANDLING – CONTAINMENT

Goal is to stabilize the environment

Consider conservative operations steps when abnormal or potentially unsafe conditions are identified

Make a backup of the systems for analysis
- A binary backup, NOT a full or incremental backup

An incident handler should not make things worse

Secure the area

Physical versus virtual containment

Change passwords locally

Okay, we have spent countless hours preparing for the eventuality of an incident. We have a good idea of what it takes to identify an incident, but where do we go from there? Being able to identify an incident solves only part of the problem. We are still left with the task of isolating and eliminating the source of the incident. This section discusses some steps that can be taken to contain an incident and, hopefully, limit its damage to the organization.

The primary responsibility of the incident handler is to make things better while adhering to the basic principles of liability and negligence. Negligence for failure to meet a certain standard of care is generally determined by a court of law. Specifically, negligence is defined as, *"the failure to exercise the degree of care expected of a person of ordinary prudence in like circumstances in protecting others from a foreseeable risk of harm in a particular situation."* In other words, a handler is responsible for meeting the expectations of the prudent person rule. Typically, a company that acts reasonably or with due care generally will not be found negligent. When an abnormal condition presents itself and there is potential for an impact to operational equipment or facilities, the incident handler needs to communicate with operations management to determine if conservative operations or other response actions are necessary.

There exists a potential for incident handlers to run into trouble while performing their duties. It is extremely important to keep in mind that there is no aspect of incident handling that allows handlers to break the law. For example, if you suspect someone within your organization of downloading child pornography, you can't download these files to your computer to examine them. Also, a handler needs to exercise due care with regard to a person's privacy under the Electronic Communications Privacy Act.

For instance, if you are an Internet Service Provider, you cannot just release the personal information of a subscriber simply because someone claims they were attacked from the subscriber's IP address.

You should also be aware that corporate officers within your organization might be held liable for your actions if they are considered unlawful.

In containing an incident, you must first secure the area. In doing so, a forensically sound backup should be made of all infected systems. If the original hard drive cannot be kept for evidence, multiple copies of the backups should be made for future analysis, if needed. One copy should be kept for evidence and the other copy used to analyze the incident. At some point in the containment process, a decision needs to be made of whether the systems should be pulled off the network or if the entire network should be disconnected from the internet. Also, passwords should be changed as soon as possible to make sure a compromised account couldn't be used for re-entry into the system by a remote attacker.

One of the key aspects of the incident handling process is to be able to present, with a high level of detail, the different pieces of evidence found and all the actions performed during the whole process. For this purpose, you should take detailed notes of all the events associated with the incident, from the Identification (step 2) to the Recovery (step 5) phase, preferably using numbered paper notebooks.

INCIDENT HANDLING – ERADICATION

Fix the problem before putting resources back online

Determine the cause, not the symptoms

Identify and remove backdoors

Improve defenses

Perform vulnerability analysis

Make sure reinfection does not occur

Before the system goes back online, an incident handler must make sure that he/she fixes the problem or the vulnerability that the attacker used to compromise the system. At first glance, the tendency may be to wipe out the entire operating system and rebuild it from scratch. Although this is certainly an effective way to remove any malevolent code, the opportunity for reinfection via the same channel still exists. There are a myriad of cases where systems were taken offline, rebuilt, and put back on the network only to be compromised again within minutes or hours. This is because a root cause analysis wasn't performed to determine why the incident happened in the first place.

It is not enough to simply recover the system and put it back online: The underlying security mechanisms of the affected systems must be altered, fixed, or upgraded to accommodate any new vulnerabilities. If it is a production system, you may hear voices of dissent from the organization about modifying a server running on a production network. This is an important, and to an extent, valid argument, but the counter is that if the system were compromised, then it must contain a vulnerability that might exist on other servers and could be exploited on a continual basis until the problem is fixed. Further, manually cleaning up the damage from an incident does nothing to prevent the problem from occurring again unless the problem is accurately identified and removed, patched, or otherwise mitigated.

Attackers often try to establish additional ways of ensuring remote access to the compromised system, so they have control of it even if the vulnerability exploited originally is fixed. Such backup access methods are known as backdoors and are implemented using several methods. Some of the most common ones include a process listening on a specific port and offering shells access (without requiring authentication), creating a new user account with high privileges, and scheduling jobs that periodically run programs that open new paths to access the system. As a wide incident handler, you need to not only fix the vulnerability used during the initial system compromise but also identify and remove every additional backdoor left by the attacker.

After the system is recovered, it is a good idea to run a vulnerability scanner against the affected system to see if the problem is, indeed, fixed and that no new holes were opened in the process. A number of commercial products, such as ISS Internet Scanner, work well and produce nice-looking reports, but open source tools such as OpenVAS should not be overlooked. If your organization is on a tight budget, and you need tools that perform the task with great efficiency, then you owe it to yourself to explore the open source options available.

To sum up, your main goal as an incident handler is to make sure that a new compromise using the same, or even a similar, vulnerability does not happen again.

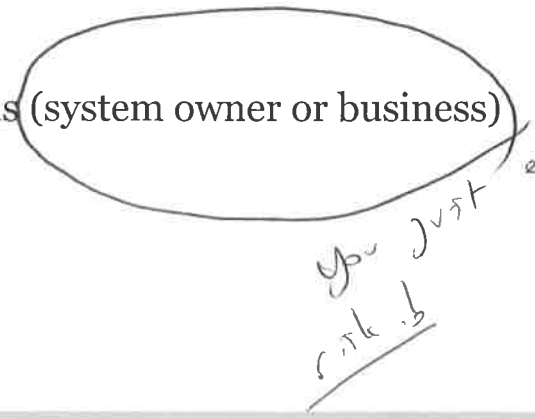
INCIDENT HANDLING – RECOVERY

Make sure you do not restore compromised code
- Install from original media, add updates, and restore data
- Restore a trusted backup patch

Validate the system

Decide when to restore operations (system owner or business)

Monitor the systems closely



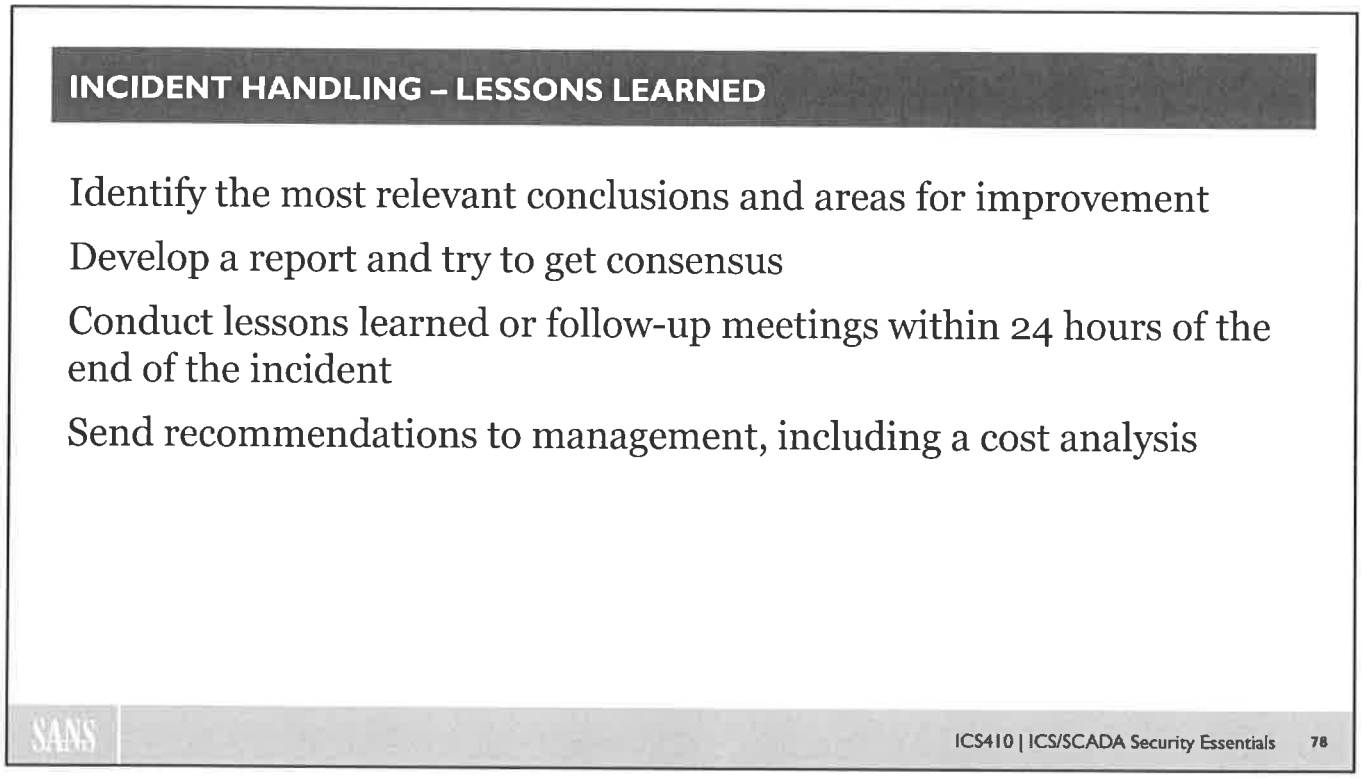
The key point to consider in the recovery phase is to ensure you are not restoring vulnerable code that has already proven itself to be exploitable by any number of attack methods. For example, if you restore a system from tape backup, then you could be restoring a previous state that contained the vulnerability exploited by the attacker. In this context, vulnerable code refers to operating system software that hasn't been patched to the latest levels, source code, and/or application software being used on the affected system.

The two main options available when restoring a compromised system:

1. Installing the operating system (OS), firmware, applications, and configurations from scratch using the official and original media, adding the latest OS and application software updates (fixing the vulnerability exploited during the incident), and finally restoring the data from a backup.
2. Restoring the system from a trusted backup and patching the system to at least fix the vulnerability involved in the incident. The trusted backup already contains the latest system and application data available.

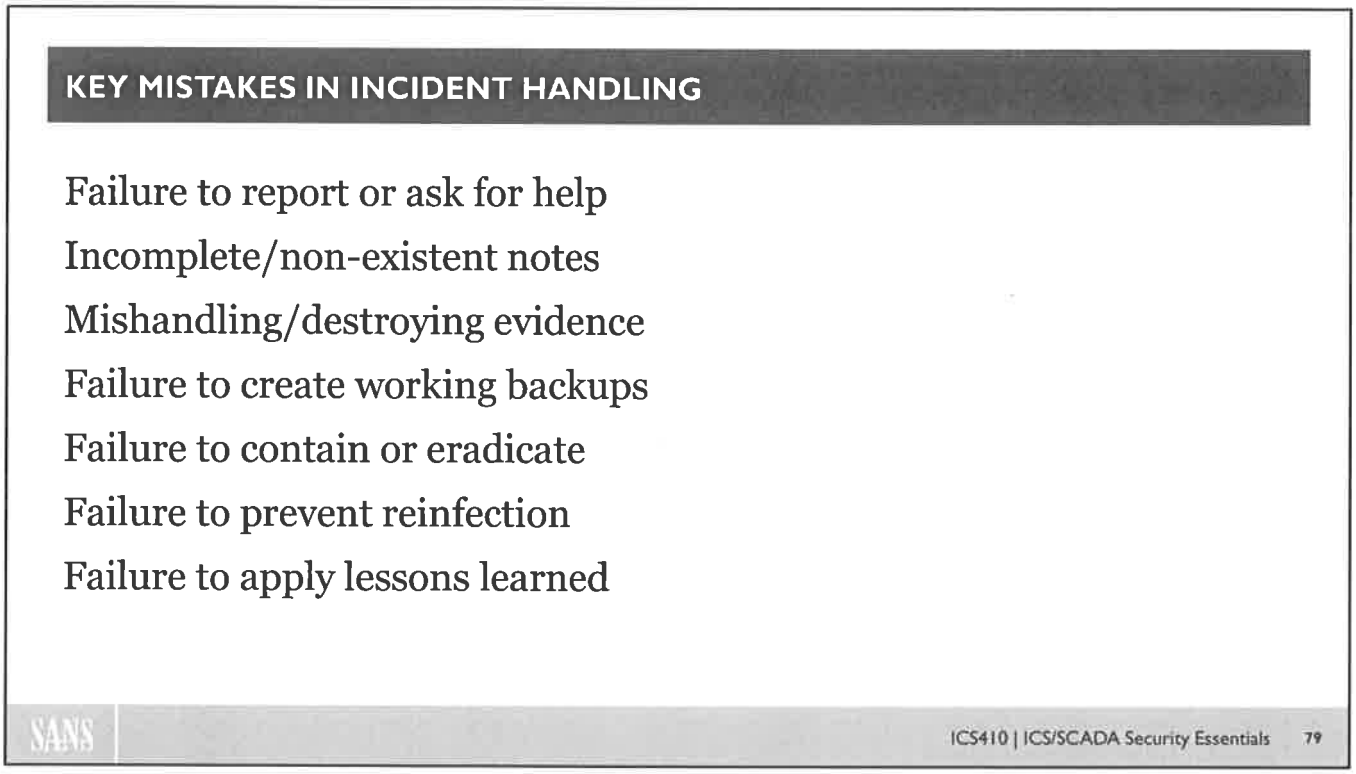
Before the system can be brought back into production, the incident handler needs to validate the system along with the system administrator. Removing the vulnerability could have affected other functions of the system that are deemed critical by the business. Anything that breaks after the recovery is likely to be blamed on the incident handler, so every effort should be made to ensure the system is working as normal before turning it over to the system administrator.

In addition, the decision on when to put the system back into production has to be made by the system owner. The handler can give advice and be as helpful as possible, but, ultimately, the final decision of bringing a system back online rests in the hands of the system owner and/or administrator. It should go without saying that if the eradication were not complete, or the infection vector were not closed off, there stands a chance of reinfection. Monitor the systems closely for the first few hours of operation to see if anything crops up that could be attributed to the original incident. Monitoring will also help demonstrate to the organization the importance of an incident handling team, and the dedication of the team members to ensure the problem is taken care of correctly.

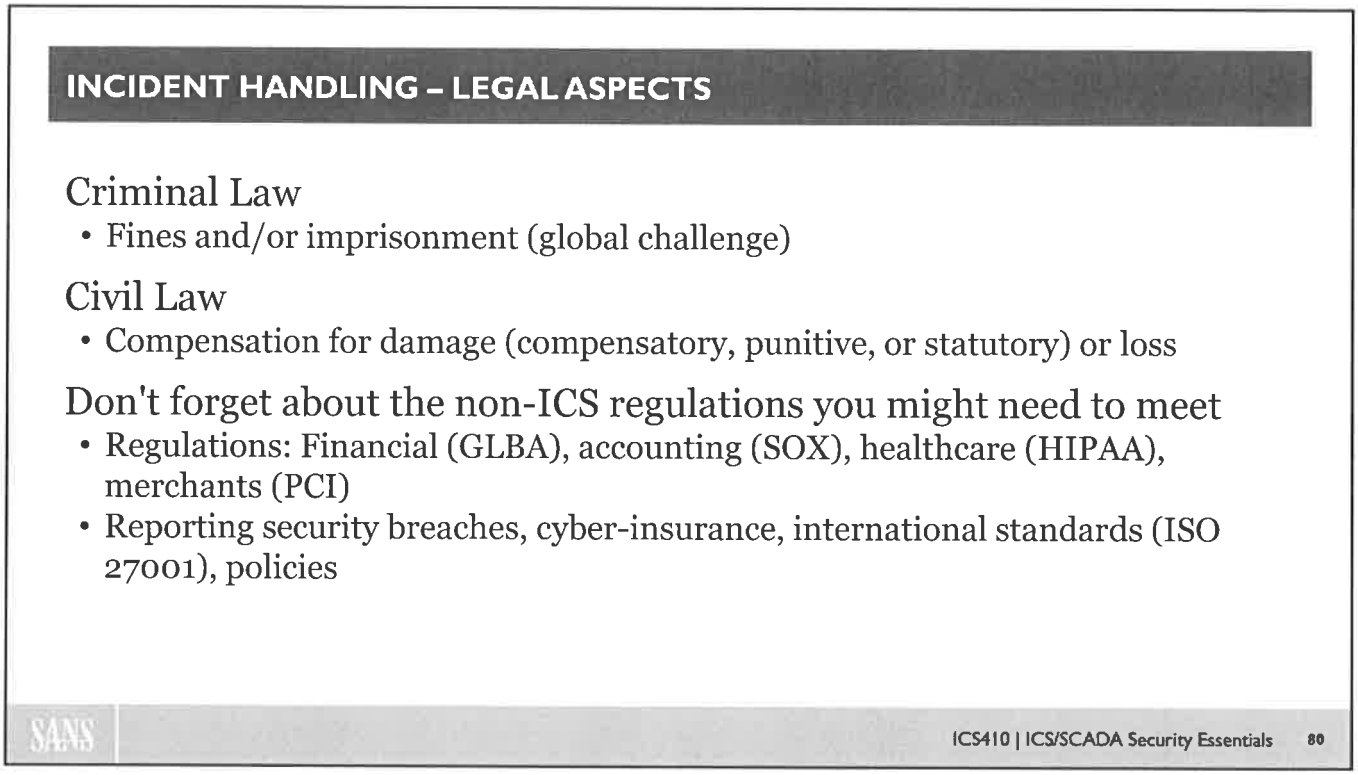


After the system has been restored and is back in operation, a report outlining the entire process should be drafted by the primary incident handler. It is important to summarize the incident, identifying the most relevant conclusions obtained to aid in avoiding similar incidents in the future. The report should contain areas for improvement, both in the security infrastructure and in the incident handling process itself. In addition, the report must point out new security actions or projects identified during the incident and that must be implemented to increase the overall security of the IT environment.

The goal should be to get consensus with everyone involved. After the report has been drafted, all members of the incident handling team should meet for a "lessons learned" overview. The goal of this meeting is to come up with a list of items that need to be included in the executive summary of the report. The executive summary should contain a brief synopsis of the entire incident, including the steps taken to recover and recommendations made.



Conducting a follow-up meeting with all involved parties is never a fun task, but it is vital to making sure the organization understands what happened, why it happened, and what steps were taken to make sure it doesn't happen again. During every incident, mistakes occur and there is a tendency to place blame. However, the goal of the follow-up meeting should be to improve the process and learn from the mistakes.



As you can imagine, the security professional needs to take many factors into account when reacting to an incident; for example, whether law enforcement should be advised, whether charges should be filed, or if a criminal offense has been committed.

Criminal law was designed to protect the public from conduct considered in conflict with certain societal norms (for example, assault, murder, rape, fraud, and more recently, computer crime). Criminal law generally imposes fines, orders the confiscation of assets (for example, the proceeds of crime, or "drug money") and/or may impose a period of imprisonment. In some countries, the death penalty may be imposed.

Certain acts may have both criminal and civil consequences. A drunk driver may be prosecuted for the crime of drunk driving and sued by the victim for damages for her injuries. Computer crime laws, such as the US Computer Fraud and Abuse Act, may contain both civil and criminal law penalties.

Computer crime has proven to be challenging for global law enforcement agencies, as the crimes are often anonymous, hard to trace, and borderless. The criminals may reside in a jurisdiction with inadequate, if any, computer crime laws. As a result, it may be impossible to extradite them. Some computer crimes may even fall between the cracks. The law attempts, with limited success, to keep pace with evolving threats. For example, international treaties, such as the Cybercrime Convention, attempt to ensure that signatories have similar computer crime laws and that international cooperation is rendered more effective.

Civil law deals with adjudicating private disputes between parties, such as neighbors fighting over noise pollution. The Law of Torts is the area of civil law that deals with many such disputes. A "tort" is simply "a civil wrong." The Law of Negligence forms an integral part of "Tort Law." Generally speaking, to be held accountable for negligence, a party must owe "a duty of care" to the injured party; there must be a breach of that duty, and damage must follow as a result of the breach.

In the security arena, damage resulting from a security breach can be hard to prove; so it is important to document the cost of all remedial measures, including the time/number of personnel spent on such efforts.

Sometimes, in certain egregious cases, or where the law allows it, the damages awarded may be punitive in nature; more than is necessary to restore the injured party to the position they were in before the breach.

In the event of an attack—malware, Denial of Service, loss of system availability, or stolen information—it is important to get legal advice to ascertain whether court orders can be obtained to try to trace and/or recover assets or get compensation from a defendant. Determined insiders may try to move stolen assets offshore. Involving legal counsel and law enforcement agencies in a timely manner may be of the essence in trying to recover them.

After the Enron scandal and other such financial and accounting scandals, many governments have adopted tough new laws and regulations to try to prevent similar incidents occurring in the future. For example, the US Sarbanes-Oxley Act (SOX) is legislation intended to reform the accounting practices, financial disclosures, and corporate governance of public companies. Certain regulated sectors, such as pharmaceutical, healthcare, and financial services, have always been heavily regulated around the world because there is a greater potential for harm to the public if something goes wrong. For example, the Food and Drug Administration (FDA) in the United States regulates the drug companies to ensure that they only develop, market, and sell "safe" products to the public; and the US banking regulators, such as the FDIC and the OCC, are required to protect the public and the safety and soundness of the banking system as a whole. International regulators, such as the Bank of International Settlements (BIS), issue rules and guidance to member banks (for example, The Basel Accord) to protect consumers and global financial markets.

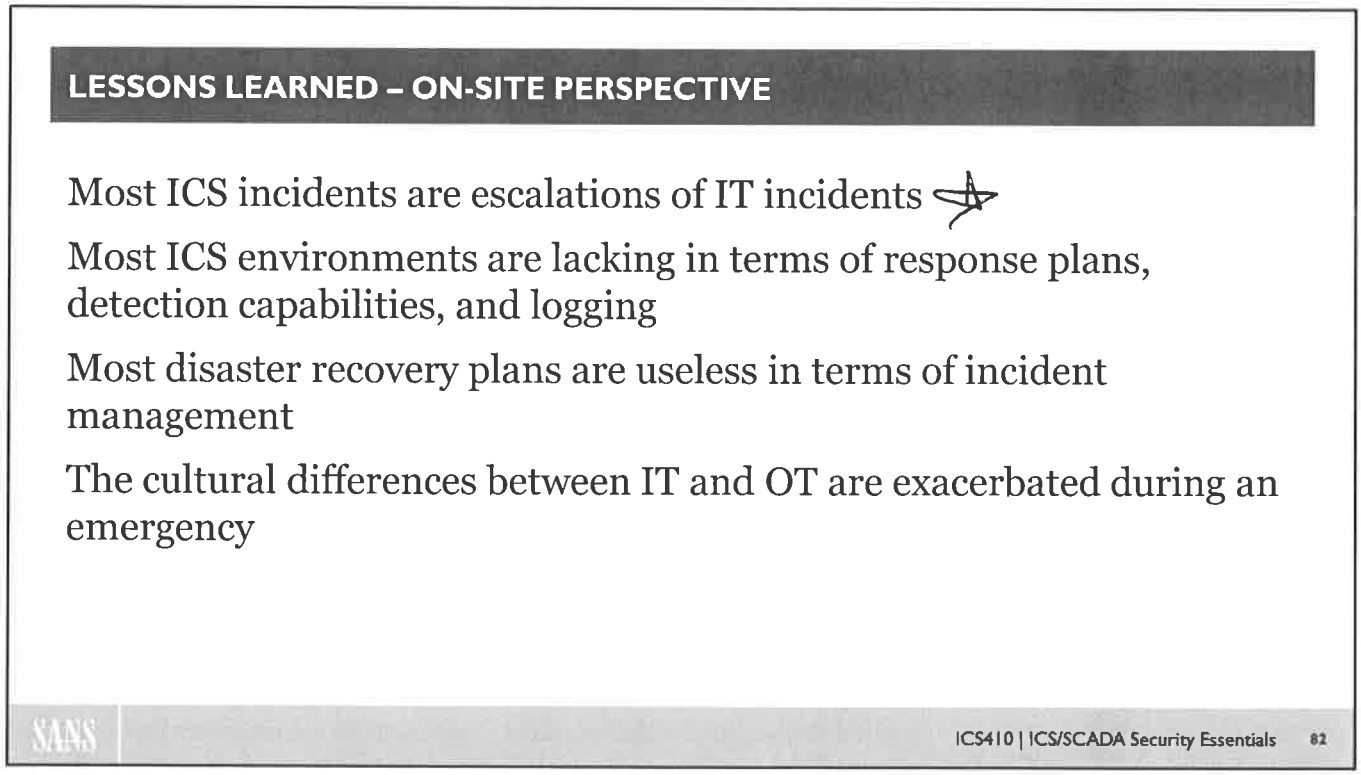
In certain regulated sectors, such as financial services and healthcare, statutes such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) may compel industry participants to adopt security policies and procedures that include incident handling and business continuity planning. HIPAA protects health insurance coverage, establishes national standards for electronic healthcare transactions, and addresses the security and privacy of health data. GLBA requires that financial institutions ensure the security and confidentiality of customer personal information against "reasonably foreseeable" internal or external threats.

There are modern regulations affecting generic sectors, such as merchants dealing with credit card information. The Payment Card Industry (PCI) Data Security Standard is an industry regulation developed by VISA, MasterCard, and other bank card networks. It requires organizations that handle bank cards to conform to security standards and follow certain requirements for testing and reporting.

Traditionally, senior management has been reluctant to report security breaches for fear of negative publicity and other adverse consequences. However, certain laws in the United States, such as SB1386 in the state of California, mandate that security breaches be reported to consumers in defined circumstances, usually where the exposed or lost data was unencrypted. Under US SEC rules, public companies are under an obligation to report to regulators if an event occurs that may impact the stock price.

If competitors or foreign governments are implicated in an attack, counter-espionage laws may be relevant. Certain countries, such as Canada, Australia, and the EU member countries, have strong privacy laws that contain security-relevant provisions that must be respected, such as the "Ley Orgánica de Protección de Datos de Carácter Personal" (LOPD), Personal Data Privacy Protection Law, available in Spain.

Investigations may also reveal illicit employee activity, such as the downloading and storage of illegal software, music, videos, or pornography on company property. Such activity may expose the company to liability and/or severe penalties. Hence, strong email and computer usage policies are essential. All employees must be fully aware of what constitutes appropriate behavior and be aware of the consequences of non-compliance.



An ICS compromise is difficult to deal with. The scenario is further complicated by the fact that few owner/operators detect the compromise themselves but are rather notified by the government, a researcher, or a firm. Few environments have the logging capabilities in place to effectively deal with incidents that happened in the past. This is especially true for incidents that occurred longer in the past than the default log rollover period on most network devices (approximately 30 days). Further complicating the confusion is the fact that many IT/OT organizations have different leadership chains and effective decision-making is completely inhibited. The skills necessary to make decisions that impact both the IT and the ICS environment are possessed by few people in an organization and in some cases, lie only in the hands of the incident responder, who is usually not well enough versed in the specifics of that environment to make the decision. Another layer that further complicates the ICS IR world is the involvement of the government. It is nearly certain that the ICS-CERT, the FBI, and potentially a federal regulating entity will be involved in the incident. It is critical to remember that the asset owner/operator is still in control, even though it may not feel that way. The government has a perspective on threats and attacks that few others can provide and this should be taken advantage of. However, they lack the resources to effectively see breaches through to the end. It is highly advised that owner/operators call an expert to help manage all aspects of the incident and to be the trusted advisor when working with the government. It is essential that this expert be chosen and vetted before an incident occurs. Each of these problems cause delays in a process where time is of the essence. Pre-emptive planning and regularly scheduled exercises can greatly increase efficiencies and make management of these incidents far easier.

Key takeaways for the IR process:

Many asset owner/operators are caught up in the media-driven attack 2.0 frenzy. Almost without fail, successful attacks are based on tried and true methodologies, many dating back to the early 2000s that a great number of ICS assets are still vulnerable to. A return to the fundamentals of security is necessary to combat sophisticated attackers.

Plan, plan, plan: Create an IR plan that holds authority for the entire organization. Use attack trees, kill chains, and any other decision criteria that fit your organization. The purpose of an IR plan is to put the power in the hands of those who can actually resolve the incident. Reporting structures and escalations are necessary and they should be well documented. TEST YOUR PLAN OFTEN.

Spend the money: The security team members in nearly every organization can provide a list of 5–10 items that concern them right off the top of their heads. Responding to an event is far more costly than preventing one. Investing in your infrastructure is the cost of doing business and spending less money sooner beats spending more money later.

Be involved: There are many information sharing mechanisms available for those in the ICS world. Awareness goes a long way; an organization that is aware of the threats and risks facing it from the operator all the way to the CEO is an organization that will work together to resolve an incident.

Lastly, you will be attacked. Your security team needs to have the tools and the training to quickly identify the level of the attack and whether it was targeted. When it comes to learning these skills, there is no substitute for experience. Invest in your people.

REGULATORY EXAMPLE OF INCIDENT HANDLING

NERC CIP-008 – Incident Reporting and Response Planning

- Process to identify, classify, and respond to cybersecurity incidents
- If you identify a cybersecurity incident
  - Determine if it is reportable
  - Notify the E-ISAC within 1 hour
- Roles and responsibilities of response personnel
- Incident handling procedures

Test incident response plan every 15 months one of three ways

- Respond to actual reportable event
- Perform a tabletop exercise
- Perform an operational exercise

Update based on lessons learned

NERC CIP-008 contains a number of requirements for organizations to develop and implement an incident response plan.

These requirements result in the development and implementation of a required plan with reporting notifications to the E-ISAC, which operates as one of the few ISACs with mandatory reporting requirements.

Incident response plans need to guide the Cyber Security Incident Response Team (CSIRT) on how to appropriately identify a suspicious event, classify the event as an incident based on analysis, and respond to the incident in a manner that ensures focus on safety and reliability. Organization plans will likely go far beyond these three items identified in the requirements and will include additional guidance for your teams to include direction on incident chain of command, individual roles and responsibilities, procedures aligned with the various phases of incident handling, and follow-up actions where appropriate.

Reference:
http://www.nerc.com/pa/stand/Pages/ReliabilityStandardsUnitedStates.aspx?jurisdiction=United%20States

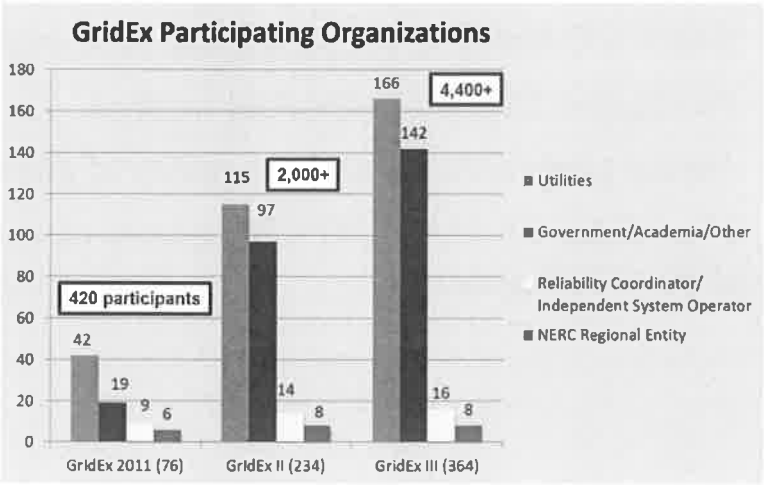
ELECTRIC SECTOR'S GRIDEX

Organized every other year by NERC

Open for all bulk power system asset owners in North America

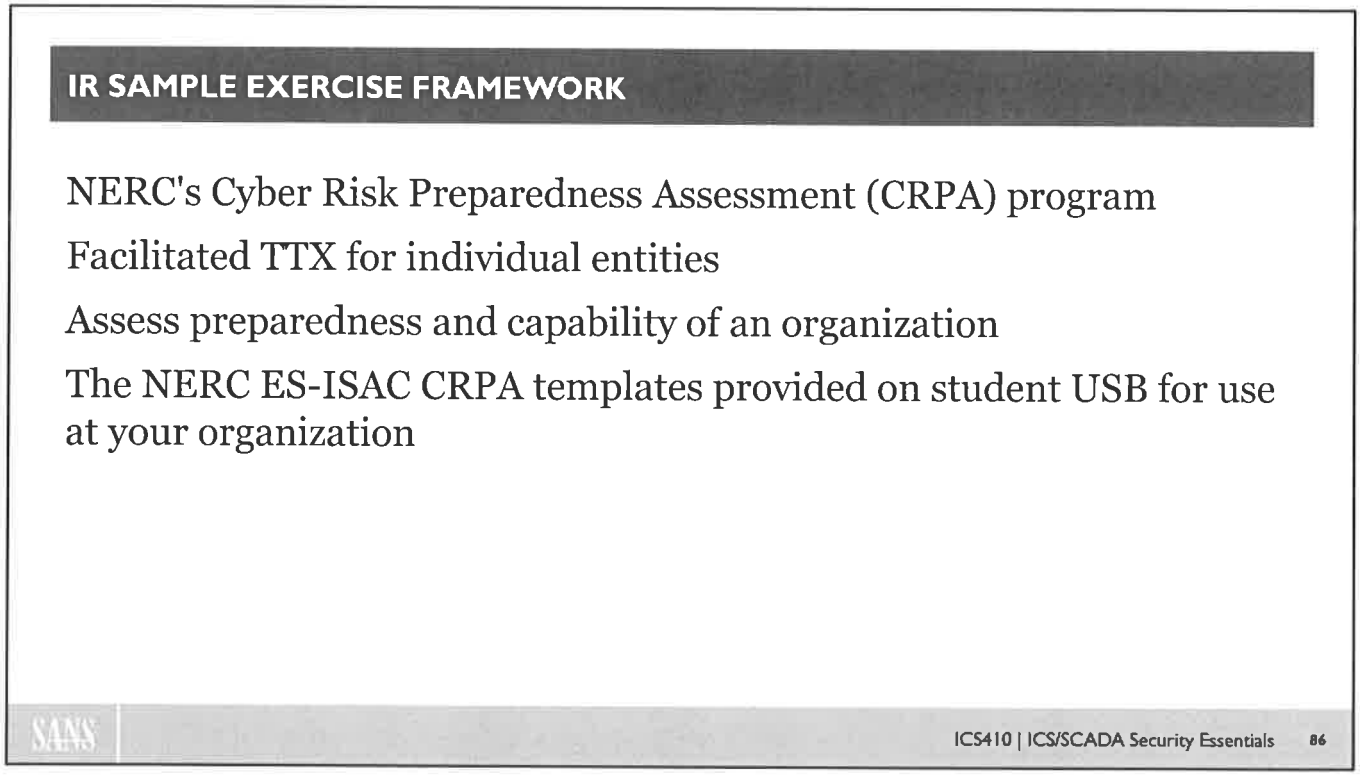
Facilitated, distributed tabletop exercise (TTX)

Full play from more than 4,400 players from asset owners, law enforcement, government, and vendor organizations



An example Advanced TTX with distributed play exercise is the NERC GridEx exercise. This exercise has been run a number of times and has defined objective sets for each exercise, which differs from the previous event. The exercise is open for all NERC registered entities, select government, vendors, and other limited third-party participation. The exercise is facilitated by a contained exercise control team that deploys the injects and overall drill communications; however, entity planners and players conduct the exercise at their normal place of work or in a large conference room at their distributed facilities.

Each year, GridEx has grown in participation and exceeded 364 participating organizations and more than 4,400 players.



The Electricity Sector – Information Sharing and Analysis Center (ES-ISAC) conducts Cyber Risk Preparedness Assessments (CRPA) of NERC Registered Entities, assessing entity capability and response to cybersecurity challenges. The CRPA is designed to assess the current cyber resiliency capabilities of bulk power system entities and the adequacy of existing reliability mechanisms related to the unique nature of cyber threats. By conducting such an assessment, NERC can focus on key improvement areas and also identify best practices (successes) to be shared with the industry.

The CRPA exercise is run as a facilitated TTX and the exercise scenarios are designed to enable the organization to assess its preparedness based on the capability to:

- Detect cyber attacks
- Prevent cyber attacks
- Respond to cyber attacks
- Manage their electronic systems and electric power assets to minimize potential damage
- Communicate and coordinate effectively with interconnected neighbors and reliability coordinators to contain the impact to the BPS
- Communicate and coordinate effectively with appropriate local and federal authorities

The NERC ES-ISAC has developed an entity starter kit that enables organizations to run their own drills. This can be found on the student USB.

INCIDENT HANDLING SUMMARY

Six-Step Process

- Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned

Tabletop Exercises (TTX)

- Benefits of exercises
- Basic exercise concepts
- Guidance and resources for building an exercise

Provided resource references for advanced hands-on exercise capability and further student development

In this module, we learned the full process involved in incident handling. Always remember that for this process to be successful, each step must be followed. The six steps that we learned are:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

Keep in mind that at some point, an incident will occur in every organization. Take a deep breath when it happens and take a level-headed methodical approach to resolving the situation. You and your organization will emerge stronger and more prepared for the next incident.

TAKEAWAYS AND RECOMMENDATIONS

Section takeaways

- Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned

Recommendations to owner/operators

- Practice your IR plans

Recommendations to vendors

- Provide a means for customers to interface with you during an incident

This page intentionally left blank.

Course Roadmap

Day 1: ICS Overview

Day 2: Field Devices and Controllers

Day 3: Supervisory Systems

Day 4: Workstations and Servers

Day 5: ICS Security Governance

1. Introduction
2. ICS Cybersecurity Programs
   - Starting the Process
   - Frameworks: ISA/IEC 62443, ISO/IEC 27001, NIST CSF
   - Using the NIST CSF
3. ICS Cybersecurity Policies
   - Policies, Standards, Guidance, and Procedures
   - Culture and Enforcement
   - Examples and Sources
4. Disaster Recovery
   - DR and BCP Programs
   - Modification for Cybersecurity Incidents
5. Measuring Cybersecurity Risk
   - Quantitative vs Qualitative
   - Traditional Models
   - Minimizing Subjectivity
6. Incident Response
   - Six Step Process
7. **Exercise 5.1: Incident Response Tabletop Exercise**
8. Final Thoughts and Next Steps
   - Other ICS Courses by SANS
   - Other SANS Curriculums and Courses
   - Netwars

This page intentionally left blank.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

DURATION TIME: 1.5 – 2 HOURS

We are going to break into groups and perform a tabletop exercise

- The instructor will present the first phase of the scenario and a list of questions
- Each group will discuss the questions within their group
- The instructor will discuss the possible answers each group came up with
- The instructor will then present the next phase of the scenario with more questions

OBJECTIVES

Tie together learnings of all 5 days of the course in a tabletop exercise

Provide students with an increased understanding of how to play and conduct a tabletop exercise

PREPARATION

Break yourselves into groups of 4–8 people

Move so you can sit as a group

For this exercise, the students can pair up or work in groups with similar focus areas (IT security, Sys Admins, Network Admins, OT, Control Sys Engineers) and provide consolidated feedback to the instructor on the various injects. Consider the talent and focus areas of your team members. In an actual response, it is essential to have developed roles and responsibilities of various members to allow for a coordinated response.

Remote students can work together via the chat capability, and on-demand students can document their thoughts before moving on to the discussion components. If the class or the instructor prefers, students can work independently and provide feedback as they are able.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 1: SUSPICIOUS TRAFFIC

You are all employed by a large chemical manufacturing company

- Your company has multiple sites around the world
- You each work on the Global ICS Security team
- You are each stationed around the world in the countries you come from

The CSO (Chief Security Officer) of the organization calls an emergency meeting

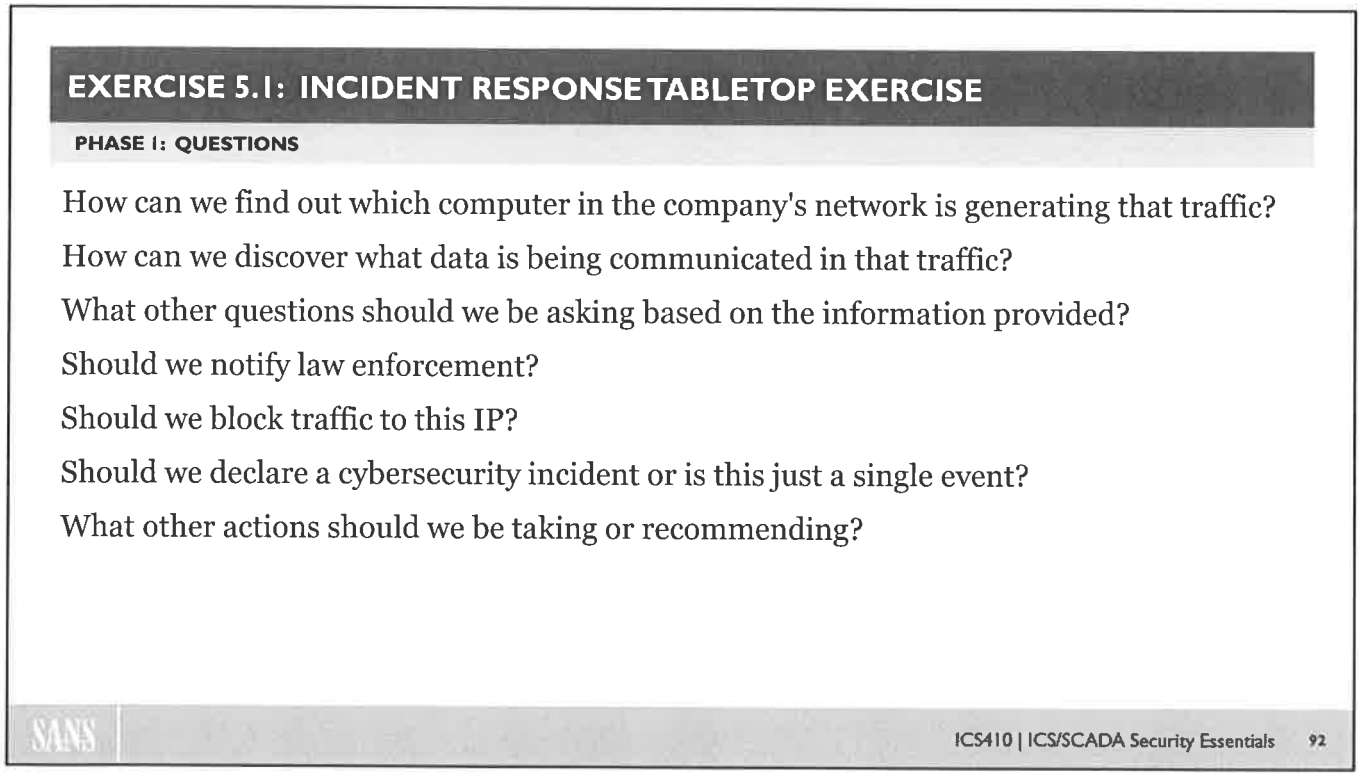
During a recent security assessment, suspicious traffic was found

- From company's IP: 66.35.59.249
- To suspicious actor's IP: 204.51.94.239
- Using TCP port 443
- Traffic is occurring Monday to Thursday
- Only occurring between 9 PM EST to 4 AM EST

During a recent security assessment, suspicious traffic was found leaving the company's IP address 66.35.59.249 and communicating with a suspicious IP at 204.51.94.239.

Multiple connections have been identified Monday through Thursday this week; however, they strangely only occur between the hours of 9 PM EST and 4 AM EST.

In many ICS organizations around the world, the local law enforcement and intelligence agencies will monitor known malicious sites and notify organizations if they see communications from their environment. For many ICS organizations, this will be the first piece of evidence they receive that a compromise exists within their environment.



It is important to consider the actions you would be taking in response to events: The policies and procedures you would use, who you would notify, and who in your organization escalates the event and has the ability to declare an incident. It is also important to always consider the actions an attacker took or the ability they have demonstrated based on the evidence you are receiving.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 2: CORPORATE IT ASSET IDENTIFICATION

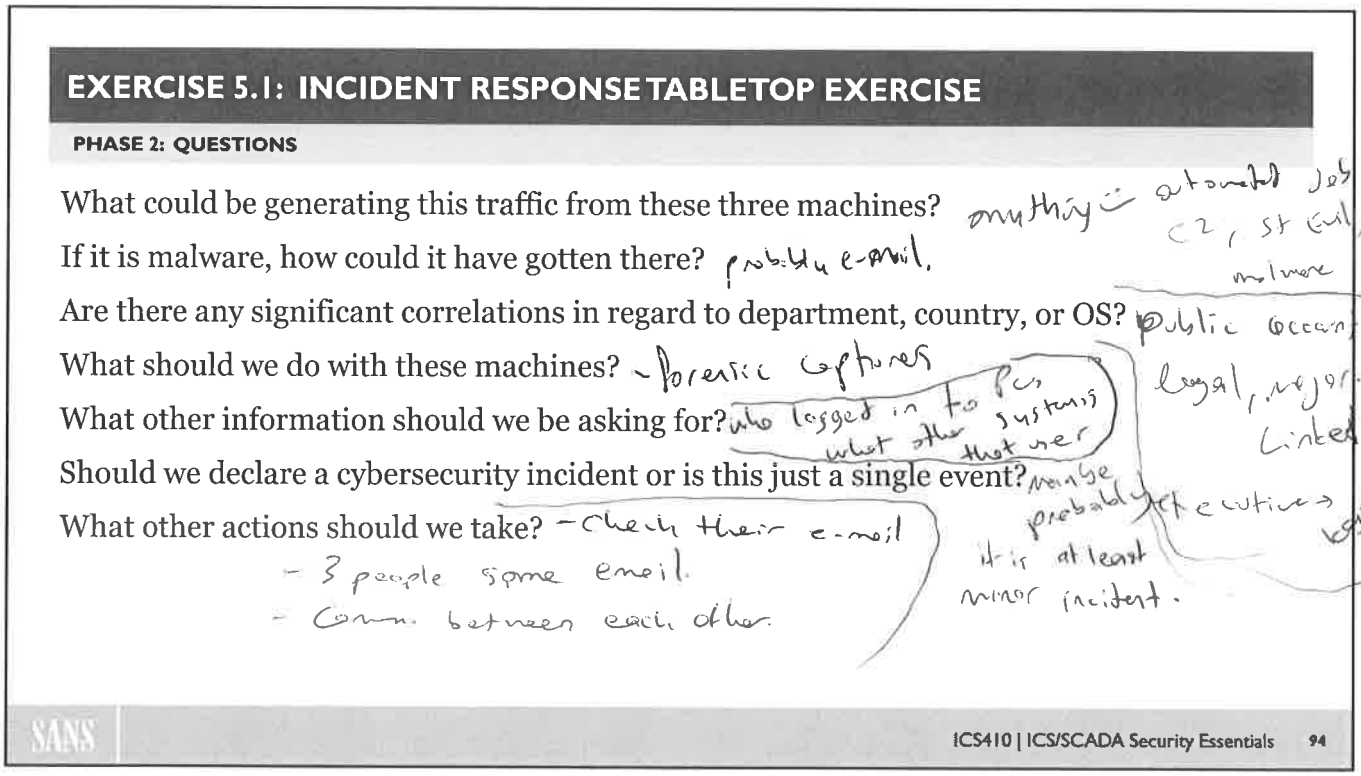
The IT team attempts to capture the traffic; however, they find it is encrypted in a TLS tunnel and not going through the web proxy

The IT team checks the NAT (Network Address Translation) logs on the firewalls

- The company's IP 66.35.59.249 is the main dynamic NAT address for the entire company
- Identify multiple hosts communicating to the malicious site (204.51.94.239)
- Originating from numerous geographic locations in a variety of subnets
- They do not store a history of any of the accepted traffic on the firewall
- They do not have a NetFlow collector or any other traffic history server

Hostname	Department	Country	Operating System
legl_w32_1024	Legal	United States	Windows XP
ma_w32_1114	Major Accounts	India	Windows XP
exc_w7_1987	Executive staff	Germany	Windows 7

Traffic going to the internet using HTTPS is often terminated through a web proxy allowing organizations to inspect and regulate the traffic; however, this must be configured for each machine in the organization or in some other way forced into the web proxy. It is common to deny all HTTPS traffic that does not go through the web proxy; however, this is not always possible with all traffic, and exceptions are often made. Web proxies are also often a point of concern regarding privacy since employees may be sending personal traffic through the business web proxy such as social networks or banking sites, which further frustrates their use.



Has anything changed in your thinking based on the new information?

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 3: CORPORATE REINFECTION

IT pulls all three machines and replaces them for the employees
- They discover your endpoint protection software was disabled on all three assets
- They perform forensics on two of the machines
- They place one in a sandboxed network with access to the internet for monitoring

One of the originally impacted users becomes reinfected on the replacement PC
- AV is disabled again
- Starts communicating out to the same malicious site

IT security forensics discovered a phishing email was the infection point
- Contained a malicious PDF that reinfected the PC
- The message was also sent to a dozen other employees in various departments
- Other personnel from other organizations were also included in the phishing email

Sometimes when machines are reinfected, it is useful to ask the employee a few questions:

Has the asset been used in other networks?
Has the user connected any removable media recently?
Has the employee installed any software?
Has someone else used the asset?
Have any new assets been connected to the device?

Many modern email servers such as Microsoft Exchange have the ability to determine which users have read certain emails, and can pull unread emails from email clients before they are read.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 3: QUESTIONS

How do you think the attackers got the emails for these specific users?

What should we do with the malicious PDF? analyz-

What actions should we take with the email and the other users who received it? pull back

What, if any, action should we take concerning the third-party organizations?

What other actions should we take?

What other information should we be asking for?

Is this an incident or a larger event than previously thought? Yes.

Has anything changed in your thinking based on the new information?

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 4: LATERAL MOVEMENT

You provide your endpoint security vendor with a sample of the malicious PDF
- Your own team starts to analyze the PDF in a sandboxed environment
- You immediately verify it shuts down endpoint software and communicates with 204.51.94.239

IT security discovers even more compromised machines
- Confirms that employees of these machines DID NOT receive the emails
- All are communicating with other IP addresses in the 204.51.94.0/24, not 204.51.94.239
- There is no trace of the PDF on these machines, but logs show logon types 3, 4, 5, and 10

Hostname	Department	Country	Operating System
rd_w7_138D	R&D	United Kingdom	Windows 7
nwk_w32_0012	Networking	India	Windows XP
eng_w7_9684	Engineering	Germany	Windows 7
nwk_2008_ema1	Networking	United States	2008 Server
eng_w32_7631	Engineering	Netherlands	Windows 7

SANS ICS410 | ICS/SCADA Security Essentials 97

ICS

Windows event logs keep a record of login attempts. Windows logon types:

Logon Type 2 – Interactive
You'll see type 2 logons when a user attempts to log on at the local keyboard.

Logon Type 3 – Network
When a user accesses a computer on the network, such as connections to shared folders or printers.

Logon Type 4 – Batch
When Windows executes a scheduled task, the Scheduled Task service first creates a new logon session for the task so that it can run under the authority of the user account specified when the task was created. When this logon attempt occurs, Windows logs it as logon type 4.

Logon Type 5 – Service
Similar to Scheduled Tasks, each service is configured to run as a specified user account. When a service starts, Windows first creates a logon session for the specified user account, which results in a Logon/Logoff event with logon type 5.

Logon Type 7 – Unlock
When a user returns to their workstation and unlocks the console, Windows treats this as a logon and logs the appropriate Logon/Logoff event but, in this case, the logon type will be 7.

Logon Type 8 – Network Cleartext
This logon type indicates a network logon like logon type 3 but where the password was sent over the network in cleartext.

Logon Type 10 – Remote Interactive
When you access a computer through Terminal Services, Remote Desktop, or Remote Assistance Windows logs.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 4: QUESTIONS

What do the logon message types indicate?

Is there any significance to the specific departments these new machines are in?

Does the greater number of external IP addresses indicate anything? Botnet ?

Is there anything important about one of the new machines being a server? Data, privilege account.

Is this an incident or another unrelated event? related.

What actions should we take? OT guys connection — local admin acc. (if some)

Who would you be notifying? ✓

SANS ICS410 | ICS/SCADA Security Essentials 98

Has anything changed in your thinking based on the new information?

Once an adversary has a foothold in a corporate network, there is traditionally a well-interconnected environment that allows an attacker to move laterally throughout the environment from asset to asset.

After the initial infection, attackers can use the Microsoft NET.EXE command and the AT.EXE command to compromise multiple internal machines. Attackers often employ AT.EXE because, by default, scheduled tasks are run as the local SYSTEM account. In addition to built-in command-line tools, attackers may use tools like Windows Credential Editor (WCE) or mimikatz to harvest credentials on local machines. They can then use these accounts to move laterally throughout the network.

Analyzing ntuser.dat timestamps can be correlated with this intrusion activity to create a better timeline.

Use of network and directory service segmentation can be an excellent defense in limiting lateral movement or at the least identifying when it occurs.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 5: ANALYSIS OF ATTACKER ACTIONS

You decide to declare a formal incident

- Declaring an incident before this point isn't a problem (more common in EU)
- Declaring an incident after this point is...a problem

Analysis of the new compromised machines shows activity performed by the attacker

- A list of installed executables
  - WinRAR
  - Pass the Hash toolkit
  - Mimikatz
  - BlackEnergy 3
- Use of privileged user accounts between the hours of 9 PM EST to 4 AM EST
- Searches on filesystems for ICS terms such as: PLC, HMI, historian, alarm, safety, protection

ICS targeted

It is probably a good idea to cut communication between IT, or by talking to Business Ops

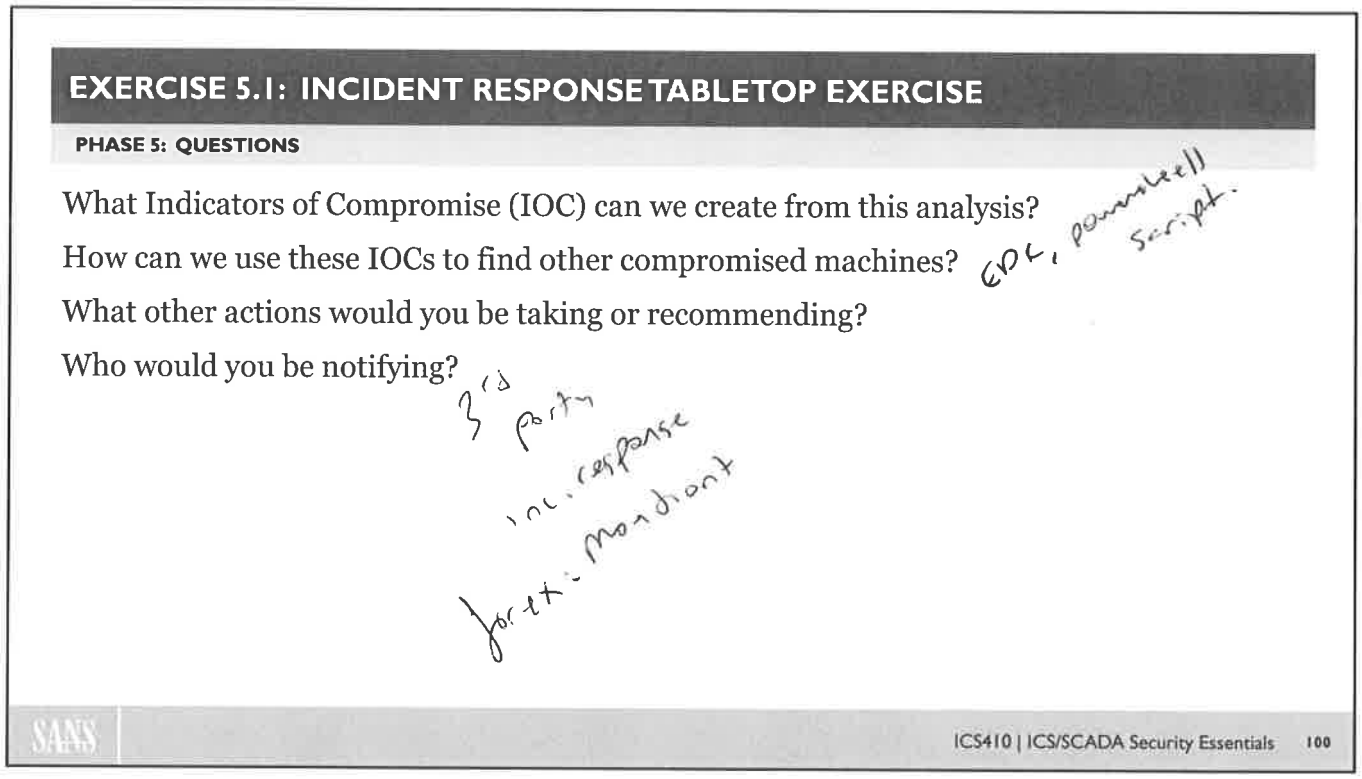
SANS ICS410 | ICS/SCADA Security Essentials 99

Mimikatz is a tool to "recover" cleartext passwords from LSASS. Why would LSASS store credentials?! Enter Digest Authentication and wdigest. wdigest is the cleartext password required to support HTTP Digest Authentication and other schemes that require the authenticating party to know the password and not just the hash.

While Black Energy 3 is one of the newer backdoors being used in the ICS, Poison Ivy offers a similar device often considered a tool for novice "script kiddies." According to experts, it has become a common feature of cyber-espionage campaigns.

The following article excerpt provides a good glimpse into the tool: "Research by malware protection firm FireEye has revealed that the tool served as lynchpin of many sophisticated cyber attacks, including the compromise of RSA SecurID data in 2011 and the 'Nitro' assault against chemical makers, government offices, defense firms, and human rights groups last year. A Peeping Tom webcam sextortionist has been jailed for six years in the US after targeting several young women in attacks that relied on a modified version of Poison Ivy, an incident that shows that the tool has malicious uses beyond cyber espionage. Poison Ivy remains popular and effective eight years after its original release."

Reference:
http://www.theregister.co.uk/2013/08/27/poison_ivy_rat_apt/



Has anything changed in your thinking based on the new information?

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 6: FAILURE TO CONTAIN

Using your new IOCs, you identify a few more machines that have been compromised

- Includes the read-only historian in the control system DMZ that the SAP servers pull data from
- These artifacts were created three days ago
- Forensics analysis indicates a strange new DLL on the read-only historian that VirusTotal says is OK

A new user "MSA1" is discovered in Active Directory

MSA1 has been added to the following AD groups

- Remote Users
- Control Operators
- Control Vendors
- Vendor Remote Access

Virus Total is a free website that scans uploaded files with a large number of different antivirus software and other threat intelligence tools attempting to indicate if the file is malicious. Some threat agents actively monitor Virus Total to identify if their custom malware is recognized as an indicator that their custom malware has been discovered, so care should be given in using Virus Total if you are attempting to prevent the attacker from knowing you are on to them. You should also be careful not to upload any file that is sensitive in nature as it releases your file into the public domain.

You can visit Virus Total at:

https://www.virustotal.com/#/home/upload

Consider group memberships access and user credentials and the impact it may have on methods of access: Web servers, Citrix environments, VPN user group, remote access groups, wireless, and even dial-up. With this level of access, there is no longer a need for internet-based command and control; however, it may still be pursued as a distractor.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 6: QUESTIONS

What do you think the attacker was attempting to do by compromising the historian?

What can you do to confirm those suspicions?

What do you think the attacker is trying to do with this MSA1 domain user?

What can you do to confirm those suspicions?

What other actions would you be taking or recommending?

Who would you be notifying?

SANS ICS410 | ICS/SCADA Security Essentials 102

Has anything changed in your thinking based on the new information?

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

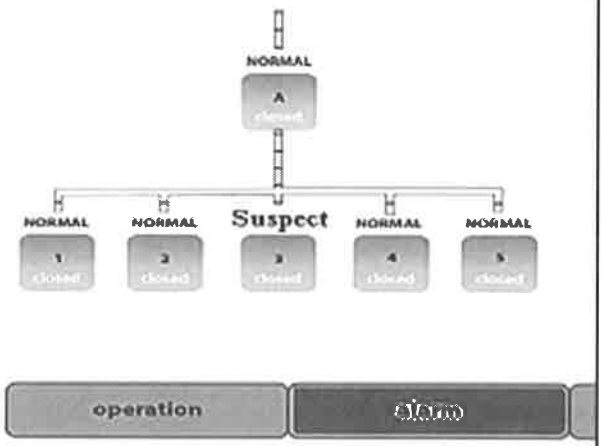
PHASE 7: STRANGE BEHAVIOR ON THE HMI

You gain permission from management to island the control network from the enterprise
You confirm there are no IOCs on master historian
You begin to review remote access logs
Operators report odd behavior in a process

- Suspect values appear on HMI
- Values disappear, then reappear changed
- Minutes later, the HMI reboots

Two alarms generated by apparent bad values

- Operator followed corrective procedure
- Indicates a condition did not exist in process
- Per protocol, operator silenced alarms and reported to management



This page intentionally left blank.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 7: QUESTIONS

What is the likelihood that the HMI event is related to the incident? probable.

If there are no IOCs on the master historian, is there any way that an attacker could compromise from read-only historian to master historian? unlikely but MB.

Since the control network has been islanded from enterprise, how could he get in? it is not isolated.

What could be causing the strange behavior on the HMI? Black energy / mTFM

Who could help us discover what went wrong on the HMI? Vendor

What other actions would you be taking or recommending?

Who would you be notifying?

SANS ICS410 | ICS/SCADA Security Essentials 104

Has anything changed in your thinking based on the new information?

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

PHASE 8: FAILURE TO PROTECT

While you were discussing those questions, you are notified that there has been an accident

- Operator that reported the strange HMI behavior has died due to an explosion
- The SIS failed to trip and protect the system

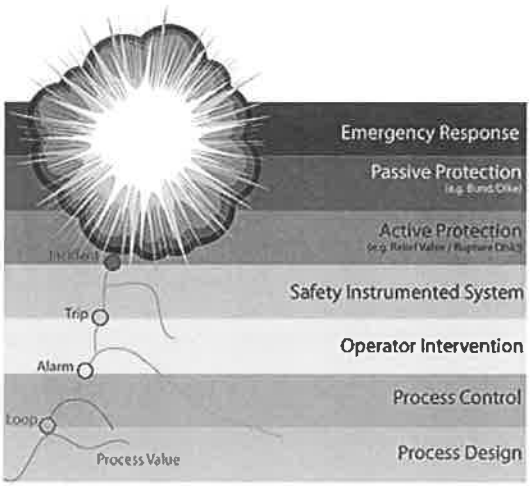
Early evidence from vendor analysis indicates

- Operator was modifying an operating parameter
- Change made was not the command received by PLC
- It is also suspected that the SIS had been disabled

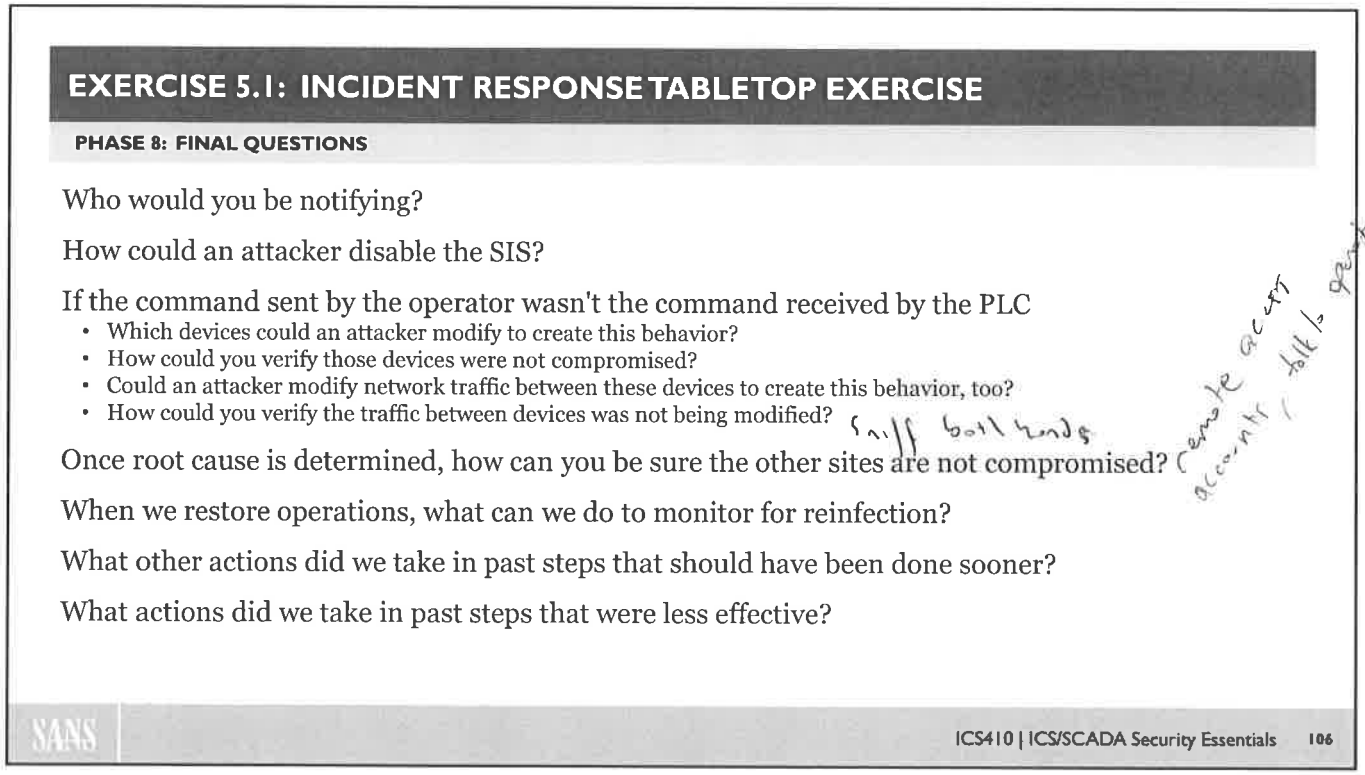
All facilities suspected of compromise have been shut down due to safety concerns

Vendors, integrators, and consultants are assembling

- Identify what went wrong
- Why the SIS failed to protect the system as designed



This page intentionally left blank.



Has anything changed in your thinking based on the new information?

Expected Player Action

Hold emergency joint security / operations meeting to discuss impacts on safety and reliable operation of the control system.

Investigate communications issues, investigate field device issues, investigate operator workstation, investigate system event logs related to connection drops (failovers, asset uptimes, network device uptimes, network connections).

Perform full analysis of network traffic internal to control network.

Report to operations, leadership, control system vendor, and law enforcement for analysis.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

CONCLUSION: UNDOCUMENTED REMOTE CONNECTIVITY HAS BEEN COMPROMISED

Upon testing, other HMI/PLC pairs at this facility showed the same behavior

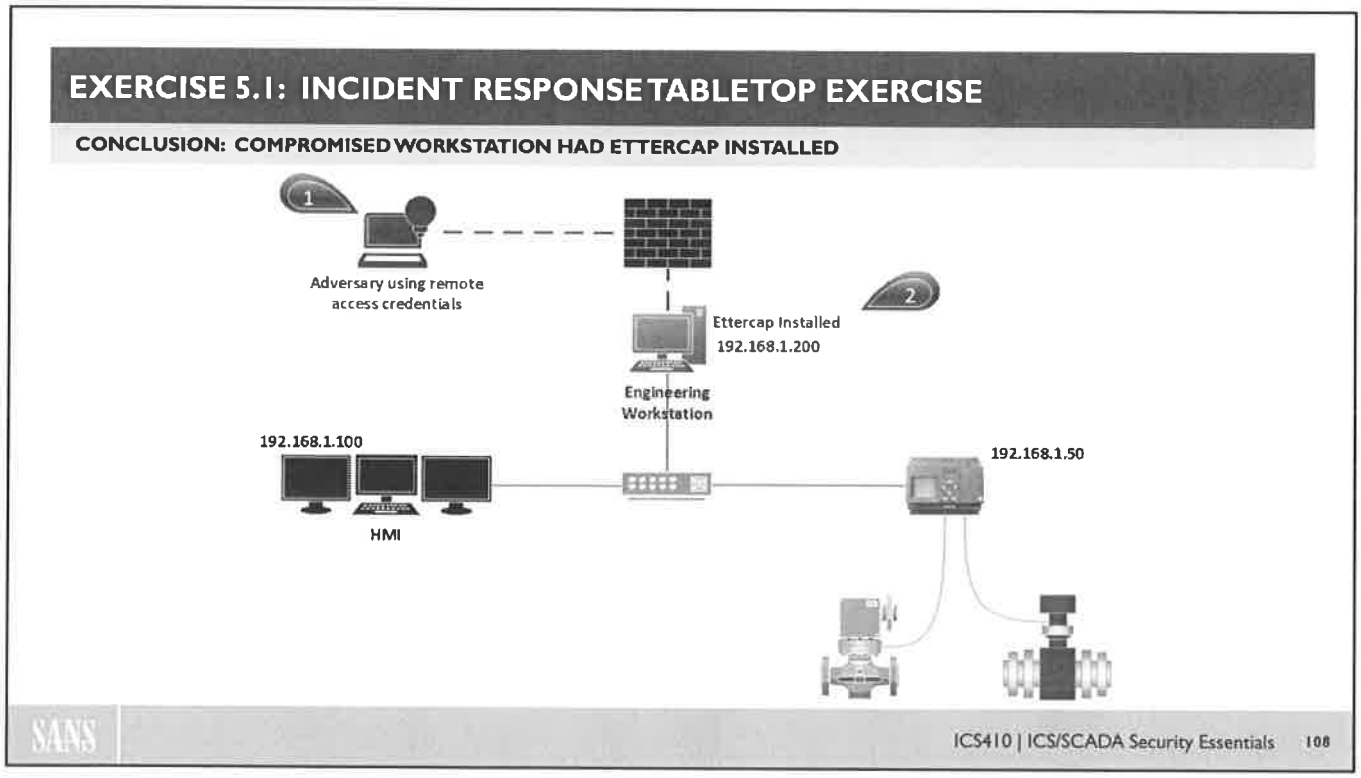
- Vendors confirm the HMIs and PLCs have not been modified
- Network captures at HMI show different packets than captures at PLC
- MAC Addresses and network switch MAC tables point to a nearby engineering workstation

Netstat is run on this engineering workstation and reports

ENG_WRKSTN TCP	192.168.1.200:44818	0.0.0.0:0	LISTENING	1688
ENG_WRKSTN TCP	***192.168.1.200:49165***	***204.51.94.234***	***ESTABLISHED***	***4***
ENG_WRKSTN TCP	127.0.0.1:445	127.0.0.1:39637	ESTABLISHED	4
ENG_WRKSTN TCP	127.0.0.1:1972	127.0.0.1:40633	ESTABLISHED	588
ENG_WRKSTN TCP	127.0.0.1:8021	0.0.0.0:0	LISTENING	1688
ENG_WRKSTN TCP	127.0.0.1:8031	0.0.0.0:0	LISTENING	1688
ENG_WRKSTN TCP	127.0.0.1:39637	127.0.0.1:445	ESTABLISHED	4
ENG_WRKSTN TCP	127.0.0.1:40627	127.0.0.1:1972	TIME_WAIT	0
ENG_WRKSTN TCP	127.0.0.1:40633	127.0.0.1:1972	ESTABLISHED	2148
ENG_WRKSTN TCP	192.168.1.200:65129	192.168.1.100:365	ESTABLISHED	3776
ENG_WRKSTN TCP	192.168.1.200:3145	192.168.1.50:535	ESTABLISHED	3786

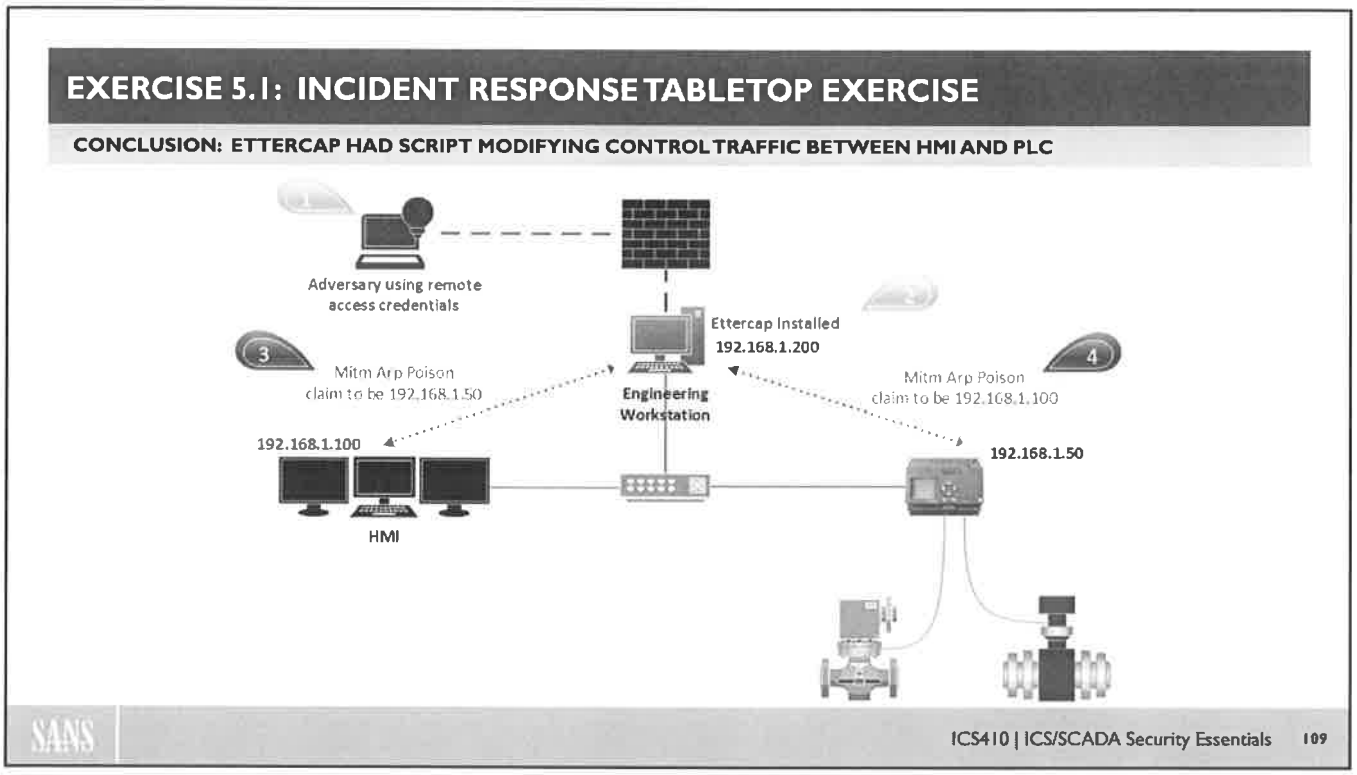
Engineers report this workstation is used by a vendor for remote access, but it is not on your maps

This page intentionally left blank.



After gaining escalated privileges and access to the directory service administration, the adversary obtained credentials for remote vendor support. The adversary then connected to the engineering workstation via RDP and installed Ettercap.

Ettercap is a tool that can be used for a number of attacks.



Selecting the MITM ARP poison attack from Ettercap, and entering in target asset 1 of 192.168.1.100 and target 2 of 192.168.1.50, Ettercap then sends an Address Resolution Protocol (ARP) update to 192.168.1.100 and says if you want to talk to 192.168.1.50, communicate to this MAC Address (entering the MAC Address of 192.168.1.200, the engineering workstation) and then performs the same to 192.168.1.50 by sending an ARP update stating that if you want to talk to 192.168.1.100, communicate to this MAC Address (again entering the MAC Address for 192.168.1.200, which is the engineering workstation). This approach places the engineering workstation in the communication path between the two targets when they talk to each other but does not impact their capability to talk to other assets.

The attacker can simply capture traffic in this position, modify traffic, generate traffic, or stop the communication altogether. Based on the reported events, it appears the attacker did not modify any traffic from the PLC to the HMI; however, when an operator sent a control signal, the attacker modified it and caused an operational event.

EXERCISE 5.1: INCIDENT RESPONSE TABLETOP EXERCISE

TAKEAWAYS AND RECOMMENDATIONS

Section takeaways

- Entry point identified
- Attack contained
- Access eradicated
- Facilities restarted
- More cleanup remains on the corporate networks, for IT to handle...

Recommendations to owner/operators

- Perform a similar tabletop exercise in your own organization
- Start small with your ICS Security team
- Include more departments on the second run

This page intentionally left blank.

Course Roadmap

Day 1: ICS Overview

Day 2: Field Devices and Controllers

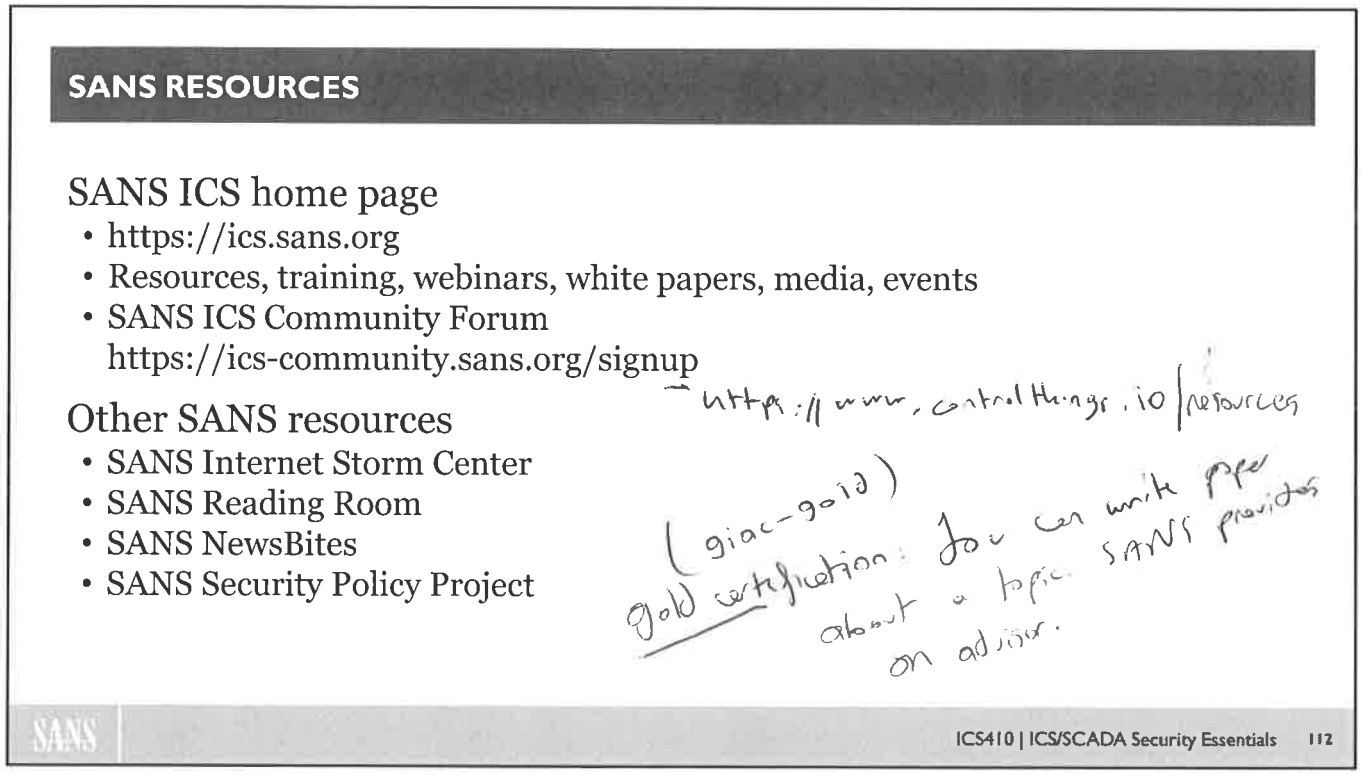
Day 3: Supervisory Systems

Day 4: Workstations and Servers

Day 5: ICS Security Governance

1. Introduction
2. ICS Cybersecurity Programs
   - Starting the Process
   - Frameworks: ISA/IEC 62443, ISO/IEC 27001, NIST CSF
   - Using the NIST CSF
3. ICS Cybersecurity Policies
   - Policies, Standards, Guidance, and Procedures
   - Culture and Enforcement
   - Examples and Sources
4. Disaster Recovery
   - DR and BCP Programs
   - Modification for Cybersecurity Incidents
5. Measuring Cybersecurity Risk
   - Quantitative vs Qualitative
   - Traditional Models
   - Minimizing Subjectivity
6. Incident Response
   - Six Step Process
7. **Exercise 5.1: Incident Response Tabletop Exercise**
8. Final Thoughts and Next Steps
   - Other ICS Courses by SANS
   - Other SANS Curriculums and Courses
   - Netwars

This page intentionally left blank.



SANS conveniently hosts quite a bit of information that will be useful to any security practitioner. Some excellent resources:

- SANS Reading Room – http://www.sans.org/reading_room/
- SANS NewsBites – http://www.sans.org/newsletters/newsbites/
- SANS Security Policy Project – http://www.sans.org/security-resources/policies/
- SANS ICS Cybersecurity Poster – https://www.sans.org/media/industrial-control-systems/ics-target.pdf
- SANS ICS Community Forum signup page – https://ics-community.sans.org/signup

ICS COURSES OFFERED BY SANS

Course	Certification	Days
ICS410: ICS/SCADA Security Essentials	GICSP	5
ICS456: Essentials for NERC Critical Infrastructure Protection	GCIP	5
ICS515: ICS Active Defense and Incident Response	GRID	5
HOSTED: Assessing and Exploiting Control Systems	—	6
HOSTED: Critical Infrastructure and Control System Cybersecurity	—	5

This page intentionally left blank.

OTHER CURRICULUMS AT SANS

Cyber Defense
- 12+ courses, 9+ certifications

System Administration
- 5+ courses, 5+ certifications

Digital Forensics Investigations and Media Exploitation
- 10+ courses, 7+ certifications

Penetration Testing
- 18+ courses, 9+ certifications

Incident Response and Threat Hunting
- 9+ courses, 8+ certifications

Management
- 12+ courses, 7+ certifications

Secure Software Development
- 9+ courses, 4+ certifications

Audit
- 3+ courses, 2+ certifications

Intrusion Analysis
- 8+ courses, 8+ certifications

Cyber Guardian
- 8+ courses, 8+ certifications

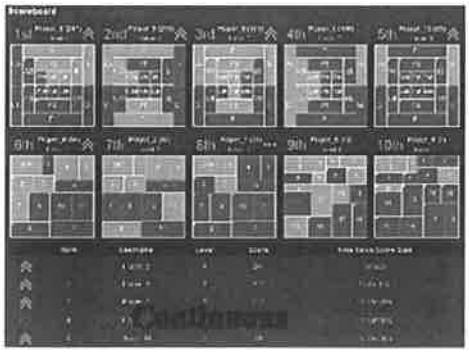
Legal
- 1+ course, 1+ certification

This page intentionally left blank.

NETWARS

NetWars is available in two forms:

- Tournament play: 1 to 3 intense days, useful to evaluate performance and learn
- Continuous play: Played at will over 4 months, more scenario-driven, useful as both a learning and practice tool, regularly updated



NetWars is designed to be accessible to a broad level of player skill ranges:
From novices up to grand masters of information security
Players can quickly advance through earlier levels to the level of their expertise

Different NetWars games across the InfoSec spectrum:
Core NetWars
DFIR NetWars
Cyber Defense NetWars
ICS NetWars

The chart at right shows the progress of the top 10 players, while the bottom shows the current score and momentum (green shows those moving up the charts, red shows downward momentum, and yellow means that they haven't changed slots recently) of the top 10 players.

SANS NetWars support finding people with information security aptitude, skills, and experience. They also provide opportunities for continual skill development in multiple disciplines in a fun and engaging fashion. NetWars, in particular, provides in-depth scenarios so that participants can directly demonstrate their capabilities and includes a scorecard showing areas for additional skill development.

"We were very impressed with SANS NetWars. The material is relevant and educational, and the tournament style play is remarkably engaging. I really like the scoring system and scoreboard."
—Adam Tice, Lockheed Center for Cyber Security

Reference:
https://www.sans.org/netwars

This page intentionally left blank.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Z