Cyber Security
Internal Audit Approach

AGA-EEI
2016 Internal Audit Training
August 23, 2016
About Cyber Security and What Has Changed
About Cyber Security

Cyber criminals are actively profiling organizations and developing highly customized malware code and attack techniques that are designed to leverage weaknesses in an organization’s security posture, that are then used to compromise systems, disrupt service and or commit fraud. Organizations are constantly assessing their security controls and security program initiatives to determine if they are able to mitigate the risk associated with these threats and potential attacks.

Internal audit, a key component of an organizations risk management activities, has an important role to play in understanding and mitigating the risks that cyber attacks pose.

The IIA’s recent cyber security white paper identifies cyber security as a board issue and defines the role that IA plays.
Industry Threats

**Electric Sector Entities Are Targets** - Electric utilities and their vendors are targeted for critical operational infrastructure. Landmark attacks like Metcalf substation, the Dragonfly APT campaigns, the recent Ukrainian grid attack and the Bowman Avenue Dam demonstrate the threat.

**Energy Sector is a Primary Focus for Cyber Attacks** - In 2014, the ICS-CERT responded to 245 incidents - the biggest share of which (32%) were in the energy sector. (According to Verizon 2015 Data Breach Investigations Report - Energy and Utilities: Critical Infrastructure)

**Prepared for the Cyber Threats?** According to 2014 Strategic Directions: U.S. Electric Industry, a report by Black & Veatch, 48% of electric utilities surveyed said they do not have the “proper segmentation, monitoring and redundancies” needed to protect against cyber threats.

In the past 5 years, there have been more targeted threats to utilities, including BlackEnergy, Stuxnet, Shodan, and Havex.

Source: ICS CERT
Note: Incidents September 2014 to February 2015

Copyright © 2016 Deloitte Development LLC. All rights reserved
The following table highlights industry threats for NYPA to protect against and manage.

<table>
<thead>
<tr>
<th>IMPACTS</th>
<th>Nation States</th>
<th>Insiders / Partners</th>
<th>Organized criminals</th>
<th>Hacktivists</th>
<th>Skilled individual hackers</th>
<th>Competitors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threats to life safety (OT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory (NERC CIP)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Destruction or degradation of cyber assets and infrastructure - OT</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial theft, loss, or fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclosure or the theft of intellectual property</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business disruption</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threats to life safety (Non-OT)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclosure, ransom or corruption of data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reputation damage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial theft, loss, or fraud</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disclosure or the theft of intellectual property</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**INDUSTRY KEY**

- Very high
- High
- Moderate
- Low

Copyright © 2016 Deloitte Development LLC. All rights reserved
Cyber – Critical Infrastructure

Based on E-ISAC’s 2016 mid year report, there is a wide range of cyber attacks the Electricity Subsector is having to manage. The image below graphically depicts the most of the attack vectors.

Figure 10: Characteristics of Cyber Bulletins

Source: E-ISAC | E-ISAC Mid-Year Report | August 2016
Cyber – What has changed?

**Tangible assets can be attacked remotely**
- SCADA; production and control networks.
- Physical security devices: cameras; intrusion detecting systems; video recorders.

**Intangible assets can be damaged on the internet**
- Brand
- Reputation: products/services; board of directors; employees
- Digital assets: intellectual property; secret information; 3rd party data

**Organization’s security perimeter has disappeared**
- Mobility: Apps / Corporate / BYOD
- Social networks presence
- Targeted attacks working from the inside

**3.0 Attacks**
- Online: Real time
- Collaborative: hacktivists; crime organizations; nations espionage
- Complex: targeted; sophisticated; multi-vector

Copyright © 2016 Deloitte Development LLC. All rights reserved
Cyber – What has changed?

The Power and Utility sector is aware of an increased pace of cyber attacks with varying degrees of factors ranging from business disruption (Distributed Denial of Service: DDoS), large scale theft (organized crime), hacktivism, and other cyber impacts coupled with increasing scrutiny and cyber legislation.

| Cyber programs are increasingly expanding... | Although energy producers are still under great pressure to reduce costs, most energy producers in the U.S. have greatly increased their cybersecurity investments. |
| The cyber criminals are outpacing companies... | There are more frequent, sophisticated, & malicious attacks with a wider range of motives than ever before. In addition, most cyber experts agree that most organizations already have hackers already inside the organization. These bad guys have the luxury of time and tremendous creativity without constraints of law or fair play. Most energy producers have not kept up with this to better forecast and combat this. |
| Energy producers are continuously maturing in certain cyber capabilities... | There are many peer energy producers who invest heavily in cyber detection (opposed to prevention only) several years ago. Although many have good relationships with the ES-ISAC to share information, most are investing in their own capabilities to provide detection systems for improved external intelligence and building behavioral intelligence/analytics for insider threats(s). |
| Regulations are getting tougher... | US auditors and regulators directionally agree that energy producers have ineffective enterprise cyber programs because management has not been serious enough about cybersecurity. With increased regulations in regulation NERC-CIP, many energy producers have struggled to keep up with increased threats and regulation. |
| Effective Cybersecurity resources and skills are difficult to maintain... | Not only energy producers, but all companies are finding it very difficult to attract and retain talented cybersecurity personnel. There is a significant salary inflation due to very limited supply and heavy demand in a market that is already 25% understaffed. |
Cyber – What has changed?
Daily Headlines

<table>
<thead>
<tr>
<th>Source</th>
<th>Date</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>eSecurity Planet, February 2016</td>
<td></td>
<td>82 Percent of Energy Sector IT Pros Say a Cyber Attack Could Cause Physical Damage</td>
</tr>
<tr>
<td>Wired</td>
<td>March 2016</td>
<td>“Cunning unprecedented attack of Ukraine’s power grid”</td>
</tr>
<tr>
<td>SmartGridNews.com</td>
<td>May, 2016</td>
<td>Ransomware attack at Michigan Utility downplayed as “incident”</td>
</tr>
</tbody>
</table>

Increase in threat to companies in the sector

Publicized threats target industrial control systems and utilities increase in the form of campaigns like Dragonfly and Black Energy. More than 1000 energy firms and controls control systems were affected.

"[The physical attack on the Metcalf substation was] the most significant incident of domestic terrorism involving the grid that has ever occurred" in the U.S.” - Former FERC Chairman, Jon Wellinghoff
Cyber – What has changed?

Daily Headlines

- The nature of cyber security attacks has changed dramatically in recent years in terms of both frequency and sophistication.

- Potential significant business impact on the following:
  - Revenue
  - Share price
  - Regulatory
  - Costs of remediation / investigation
  - Brand / reputation

As a result, cyber security has evolved from an IT department concern to an executive level issue receiving regular airtime on audit committee agendas and in boardroom discussions as recently highlighted in a recent 2015 IIA publication:

"The overwhelming number of cybercrime incidents has forced boards to become more educated about the topic and ask strategic and thoughtful questions directed toward management and internal audit."
Cyber – What has changed?

Regulation

- Mandatory Regulatory scheme for Bulk Electric System (BES) or “The Grid” is full suite of “operationalized cyber security” requirements designed to assure the reliability of the electric grid
  - BES defined - fundamental to compliance, complicated
  - NERC (North American Electric Reliability Corporation) charged with **ensuring reliability** of the BES in North America. As the electric reliability organization (ERO), NERC is subject to oversight by the Federal Energy Regulatory Commission (FERC). Operates pursuant to FERC Enforcement authority.

- Increased focus on formal regulation at distribution level
  - New Jersey BPU Regulations
  - Connecticut Public Utility Regulatory Authority
Cyber – What has changed?
“Voluntary” to “Voluntary/Mandatory”

- Executive Order (February 2013) - Directed NIST to work with stakeholders to develop a voluntary framework to reduce cyber risks to critical infrastructure

- National Institute of Standards and Technology (NIST) - Version 1.0 NIST Cybersecurity Framework - Issued February 2014. Voluntary guidance, based on existing standards, guidelines, and practices, for critical infrastructure organizations to better manage and reduce cybersecurity risk

- Other Frameworks and Standards:
  
  - **ETSI Cyber Security Technical Committee** - Standards to increase privacy and security for organizations and citizens across Europe
  
  - **ISO 27001** - provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system
  
  - **ISO 27002** -a collection of information security guidelines that are intended to help an organization implement, maintain, and improve its information security management.
  
  - **ISA/IEC-62443** - is a series of standards, technical reports, and related information that define procedures for implementing electronically secure Industrial Automation and Control Systems (IACS)
Cyber – What has changed?
Increased internal complexity

**TECHNOLOGY**

**Aging Infrastructure & Grid Modernization**
Replacement of aging infrastructure and dated systems will result in a technology transformation – this will change the way P&U companies address cyber risk.

**Complex interconnections between systems (SCADA, Industrial Control Systems (ICS), smart grid, intelligent substations, and new customer systems) are dramatically reshaping the cyber threat landscape for the Power and Utilities Sector.**

**Cyber Security Programs**

- Internal Framework Differences
- Implementation Silos
- Resources: Focus & Allocation
Cyber Risk and Role of Internal Audit
Cyber Risk

Easy questions and difficult answers that are asked of Internal audit and management...

CEO: “I read about phishing in the news. Are we exposed?”

Board: “What is our level of resilience against these Cyber attacks?”

CIO: “Where and how much do I need to invest to optimize my Cyber capabilities?”

Business unit: “What are the Cyber threats relevant to my business?”
Role of Internal Audit – Cyber Security

Internal audit provides independent oversight over the risk and control environment – including cyber security.

- **Level 0**: Line Managers
  - Primary responsibility in ensuring adequate risk and control environment in their areas of operation

- **Level 1**: In-business control teams
  - Support the line managers, oversee the implementation of corporate and business standards

- **Level 2**: Independent / Corporate Risk & Control Teams
  - Sets policy and standards. Oversee the program from an enterprise perspective. Ensure operational risk controls are built into the business and functions

- **Level 3**: Internal Audit
  - Provide independent oversight over the risk and control environment

**Partnership with CIO and IT Risk Officer**

**Ensure clear roles and responsibilities – avoid overlaps and gaps**
Role of Internal Audit – Cyber Security

Internal audit’s role in “cyber security” is same as with other areas

Role

• Understand and assess incremental threat scenarios that expose organization to risk
• Assess controls and Identify gaps in policies, standards, processes, metrics and reporting, etc.
• Maintain “cyber security” as an organizational priority and standing agenda item in audit committee updates
• Apprise the Audit committee of key risks, enterprise level risk trends related to cyber security

So, how do you identify what should be the areas of focus for a “cyber security” audit?
Role of Internal Audit – Cyber Security
The Audit Plan – Cyber Security Audits

Topics that have been the focus of Internal Audit and new areas of cyber focus:

<table>
<thead>
<tr>
<th>Traditional Information Security</th>
<th>Cyber Leaning Focus Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entitlements management</td>
<td>Cyber governance – Policies, Controls, Structures, Management and Enforcement</td>
</tr>
<tr>
<td>Segregation of duties and ID administration</td>
<td>Security event monitoring/ Security operations</td>
</tr>
<tr>
<td>Cloud computing – emphasis on IT governance, software as a service</td>
<td>Data leakage – particularly unstructured data</td>
</tr>
<tr>
<td>Mobile application security</td>
<td>Security incident response process</td>
</tr>
<tr>
<td>Privileged user access management</td>
<td>Malware detection</td>
</tr>
<tr>
<td>Third party information security risks</td>
<td>Vulnerability management process</td>
</tr>
</tbody>
</table>
Role of Internal Audit – Cyber Security
The Audit Plan – Cyber as Audit Component

Focus generally on what “cyber security audits” are needed. Cyber plays a role in many business activities and should be integrated as a component of other audits.
Common cyber threats in Energy

It is important to understand the actual threats for specific organizations, and sometimes for individual lines of business or support functions.

- Impact to life and safety
- Impact to reliable operations
- Regulatory fines
- Customer data breach
- Loss of rate payer or board confidence
- Intellectual Property theft
- Financial loss from tampered meters
Role of Internal Audit – Cyber Security
Key Considerations

**Strategically ...**
- Does your organization have a cyber security strategy including a clear cyber governance framework? Does it differ among organizations? Are some regulatory and others not?
- How is your organization evaluating and managing cyber risk?
- Is the existing risk framework adequate to address changing threat landscape?
- How structured and well-tested are your existing incident response and crisis management capabilities? Are there differing levels of maturity?

**And tactically ...**
- What is leaving our network and where is it going?
- Who is really logging into our network and from where?
- What information are we making available to a cyber adversary?
Energy Industry Readiness

- State regulatory focus on distribution level regulation of smart grid and similar customer facing technologies.

- Replacement of aging infrastructure and dated systems will result in a technology transformation that requires a new approach to cyber security.

- P&U is the tip of the spear for other Industrial Control System (ICS) driven businesses (Natural Gas, Oil & Gas, Water Utilities, and manufacturing / processing).

- **Coordination of agencies, regulators, industry, private sector is essential.**

Security + IT + Compliance = Cyber Security

*The CIP Transition - Lessons Learned*

- Transition to CIP shows building formal compliance structures around NIST and other frameworks can mitigate risks and failures.

- Consider the IT organization and their role in cyber security and compliance programs.

- Assess how to **integrate and formalize cyber frameworks** for the implementation of programs applicable to regulated and non-regulated assets to improve cyber security posture.
Cyber Internal audit “What and How?”
Critical Assets
Assets critical to the operation / business activity

Critical Cyber Assets
Cyber assets critical to the operation of critical assets

Protection of Assets
How are we protecting critical and critical cyber assets
What: Typical areas of focus

The objective of a Cyber security audit is to provide management with an independent assessment relating to the effectiveness of Cyber security practices and controls specific to the prevention, detection and incident management processes and governance activities at the organization.

- **Cyber threat risk assessment**
  - A Cyber risk assessment could range from a half day session with select stakeholders within the organization where a generic threat catalogue is presented and discussed to help prioritize the key areas of risk OR it could take between 1-2 weeks, depending on the number of workshops, interviews, surveys, locations, business units that need to be scoped in.

- **Cyber governance, security mgmt. & security policy & enforcement**
  - Cyber security policies and standardized processes to enforce the policies throughout the organization. Cyber security goals, objectives, enforcement and scope will be assessed in this category.

- **Vulnerability & patch management**
  - Assess the ability to proactively identify vulnerabilities in the network and implement controls to mitigate the vulnerabilities.
What: Typical areas of focus (cont’d)

- **Security event monitoring**
  - Assess enterprise wide monitoring and visibility through correlation of network, host and application security events to detect malicious activities.

- **Data leak detection/prevention**
  - Assess ability of an organization to detect and restrict data leakage of confidential and corporate information.

- **Vulnerability & patch management**
  - Assess capabilities in detection and stopping malware threats including email security, web security, IDS/IPS, AV and advanced malware detection and interception technologies.

- **Incident response**
  - Evaluate the processes and technologies in place to perform incident management and response, malware analysis and cyber forensics in an effective and consistent way.
  - Evaluate process and procedures in place related to restore the capabilities or critical infrastructure services that were impaired through a cyber security event.
Deloitte’s Cyber Security Framework Components

Our cyber security framework is organized by key capability areas that cover common capabilities that are prevalent in many organizations. These capabilities areas are derived based on our experience serving clients, industry leading practices and applicable regulatory requirements.

<table>
<thead>
<tr>
<th>Secure</th>
<th>Vigilant</th>
<th>Resilient</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Application Security &amp; SDLC</strong></td>
<td><strong>Vulnerability Management</strong></td>
<td><strong>Cyber Operations</strong></td>
</tr>
<tr>
<td>Secure development lifecycle</td>
<td>Vulnerability management framework</td>
<td>Security Operations Center (SOC)</td>
</tr>
<tr>
<td>Security during change management</td>
<td>Vulnerability scans (external and internal)</td>
<td>Log correlation</td>
</tr>
<tr>
<td>Emergency change control</td>
<td>Vulnerability scoring model</td>
<td>Threat Intelligence and Analytics</td>
</tr>
<tr>
<td><strong>Infrastructure Security</strong></td>
<td><strong>Threat Intelligence</strong></td>
<td>System, network and application monitoring</td>
</tr>
<tr>
<td>Malware protection</td>
<td>Threat intelligence and modeling</td>
<td>User activity monitoring</td>
</tr>
<tr>
<td>Network and wireless security</td>
<td>Cyber profile monitoring</td>
<td>Privileged user monitoring</td>
</tr>
<tr>
<td>Network / application firewall (and recertification)</td>
<td>(including internet presence, typo squatting, social media etc.)</td>
<td>Penetration testing (external and internal)</td>
</tr>
<tr>
<td>Network admission control</td>
<td><strong>Cyber Analytics</strong></td>
<td><strong>Security</strong></td>
</tr>
<tr>
<td>Intrusion Detection / Prevention Systems (host and network)</td>
<td><strong>Incident and Event Management</strong></td>
<td>Information and Risk Management</td>
</tr>
<tr>
<td>E-mail security</td>
<td>Threat feeds and honey pots</td>
<td>Security information and event management</td>
</tr>
<tr>
<td>Key and Certificate Management</td>
<td>Brand monitoring</td>
<td><strong>Incidents</strong> and <strong>Aggregation</strong></td>
</tr>
<tr>
<td>Web Proxy</td>
<td>Insider threat monitoring</td>
<td>Fraud / AML / Physical</td>
</tr>
<tr>
<td>Remote access</td>
<td><strong>DDOS monitoring</strong></td>
<td>Operational Loss</td>
</tr>
<tr>
<td>Endpoint protection</td>
<td></td>
<td>Source / cause</td>
</tr>
<tr>
<td>Secure file transfer and storage</td>
<td><strong>Continuity</strong> Management</td>
<td><strong>Cyber</strong> Simulations</td>
</tr>
<tr>
<td>Device to device authentication</td>
<td></td>
<td>Simulation plans and schedule</td>
</tr>
<tr>
<td>Patch management</td>
<td><strong>Business Continuity and Disaster Recovery Planning</strong></td>
<td>Table top exercises</td>
</tr>
<tr>
<td><strong>Physical Security</strong></td>
<td></td>
<td>Full scale simulation</td>
</tr>
<tr>
<td><strong>Identity and Access Management</strong></td>
<td><strong>Incident Response and Forensics</strong></td>
<td>Post exercise analysis and improvement</td>
</tr>
<tr>
<td>Provisioning and de-provisioning</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authentication and authorization</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Role based access control</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Segregation of duties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Access re-certification and reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Federation and SSO</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privileged user management</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Protection</strong></td>
<td><strong>Third Party Risk</strong></td>
<td><strong>Risk Assessment and Mitigation</strong></td>
</tr>
<tr>
<td>Data classification and inventory</td>
<td>Security during selection onboarding</td>
<td>Risk based authentication</td>
</tr>
<tr>
<td>Data encryption and obfuscation</td>
<td>Security during contracting</td>
<td>Anti-fraud controls</td>
</tr>
<tr>
<td>Data loss prevention</td>
<td>Third party monitoring</td>
<td>Database security</td>
</tr>
<tr>
<td>Data retention and destruction</td>
<td>Termination and removal of assets</td>
<td>Functional ID management</td>
</tr>
<tr>
<td>Records management</td>
<td></td>
<td><strong>Trends</strong> and <strong>Analytics</strong></td>
</tr>
<tr>
<td>Developer access to production</td>
<td></td>
<td><strong>Vigilant</strong> Model</td>
</tr>
<tr>
<td>Records management</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Third Party Risk</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security during selection onboarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security during contracting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third party monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Termination and removal of assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Asset Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Classification and Labeling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Monitoring and Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resilient</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Crisis Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Crisis response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(including readiness, forensics, notification etc.)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Cyber Simulations</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Continuity and Disaster Recovery Planning</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resilience &amp; Recovery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Continuity and Availability Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Protection</strong></td>
<td><strong>Full Scale Simulation</strong></td>
<td></td>
</tr>
<tr>
<td>Data classification and inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data encryption and obfuscation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data loss prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data retention and destruction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Developer access to production</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records management</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Third Party Risk</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security during selection onboarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security during contracting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third party monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Termination and removal of assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Asset Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Classification and Labeling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Monitoring and Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resilience &amp; Recovery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Continuity and Availability Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Data Protection</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data classification and inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data encryption and obfuscation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data loss prevention</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data retention and destruction</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Developer access to production</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records management</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Third Party Risk</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security during selection onboarding</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security during contracting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Third party monitoring</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Termination and removal of assets</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Asset Management</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Inventory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Classification and Labeling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asset Monitoring and Reporting</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Resilience &amp; Recovery</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service Continuity and Availability Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
NERC CIP Compliance Framework
The following NERC CIP Compliance Framework defines the program elements necessary to implement and maintain an effective program.

**Sub Components:**
- Cyber Asset Management
- Physical Security
- Information Protection
- Systems Management
- Production Change Management
- Personnel Risk Assessment
- Identity and Access Management
- Incident Response
- Security Information & Event Management
- Vulnerability Management
Defining Protected Information

Defining and Prioritizing Information Protection Controls

- **What** information to classify and protect
- **Who** creates, obtains, shares, stores the information
- **Where** is the information located
- **When** to implement, assess and update
- **Why** restrict access and protect information
- **How** do failures occur

Information Classification Challenges and Considerations

- Interpretation and definition
- Regulatory enforcement
- Risk based approach
- Shifting landscapes (regulatory, business, risk)
Cyber / Electronic Access vs. Physical Access

Restricting Electronic Access to Information

Managing Sharing, Storage and Transmission

Restricting Physical Access to Information

Destruction of Information

Copyright © 2016 Deloitte Development LLC. All rights reserved
Cyber Internal Audit “Where Do You Go From Here?”
“Where do you go from here?”

Scoping out your Cyber Internal audit reviews will depend on some key aspects that will drive the approach to be followed. The following are some of the questions that Internal audit needs to think about when scoping the reviews:

- What is the current state/ maturity and understanding of your Organization’s Cyber program or approach to cyber security?
- What is driving these Internal audit reviews?
- What are the current timelines to assess or implement the Cyber program and what is the budget that is available?

The following slides represent 2 different approaches to get started with your Cyber Internal audit reviews.
Approach 1 – Threat risk assessment

The following points act as key indicators. This approach might be a good starting point for your Cyber Internal audit reviews:

1. Internal audit would like to engage with the different stakeholders at the organization to understand and assess the current threat landscape that is facing the organization
2. Internal audit does not have a good grasp on the current state of the organization’s security program or key risk areas within that program
3. The need to conduct Cyber audits are driven by what is in the news or potential areas of risk within the industry or the audit committee’s/ board’s concern or questioning of the state of Cyber security within the organization
4. The need to understand the key areas of Cyber risk and focusing on those areas of higher risk based on defined threat risk criteria, prior to selecting the areas for audit
5. More time to perform this analysis and sufficient funding available to support the completion of the risk assessment

A good starting point to understand the current Cyber threat landscape at your organization would be through conducting a Cyber threat risk assessment.
Approach 1 – Threat risk assessment (cont’d)

A Cyber threat risk assessment is a point in time assessment of the risk the organization is facing based on the business and the environment.

**Identify critical assets**
- Create an inventory of critical assets from both a business and security/vulnerability perspective:
  - Systems
  - Data/Information
  - Communication Channels

**Assess impact of loss**
- Assess the impact of the loss of the critical asset
- Both business (regulatory/impact to business/3rd party) and CIA impact considered

**Define risk Ranking**
- Define the threat risk rating based
- Level of threat risk (HML) allows for planning of IT controls and related remediation along with related resource planning.

**Rank threats and vulnerabilities**
- What are you protecting the asset from?
- Based on threat catalogue.
- Includes human and non-human factors
- Perform vulnerability scan
- Customized for your environment

The Cyber threat risk assessment allows you to consider the Company’s cyber capabilities and help target those areas of highest risk for your audit (Cyber categories within the Deloitte Cyber security framework, slide 17).
Approach 2 – Themed audits

The following points would lead to a conclusion that a Cyber threat risk assessment might not be necessary but rather a focused (themed) audit might be the right approach:

1. Internal audit have a good grasp of the current security program within the organization and would like to assess certain aspects of the current Cyber security practices in place
2. There is no Cyber program at the organization, however Internal audit would like to assess the fundamental aspects of security that would help pin point initial areas of risk that can trigger further Cyber reviews
3. The audits are driven by potential or known areas of risk within the industry or recent intrusions or threats that have faced the company.
4. The audits are of non-cyber but the company is looking to integrate cyber components.
5. Key stakeholders (including the audit committee or board) might want to focus on key areas within security (e.g. Are we equipped to respond to a Cyber attack?)
6. The need to perform the audits within a short time frame and with limited funding/ budgets (typically 38 week reviews and could start from $40K (for 4 categories under the Cyber security framework), however can go over $200K, depending on the complexity of the business and the business units selected under the review)

The following slides will help explain how to approach a themed Cyber Internal audit review.
Approach 2 – Themed audits - Defining scope

The Cyber security framework below represents the different categories of risk and audit focus that fall under the three domains listed below (secure, vigilant & resilient). First select the domains and categories to focus on based on Internal audit’s understanding of the business and stakeholder input.

- Secure
  - Cyber security governance
  - Policies and related standardization and enforcement
  - Network Security and segmentation
  - Cyber risk management
  - Identity and access management
  - Fraud management program
  - Supply chain security
  - Operating Systems Hardening
  - Network operations

- Vigilant
  - Cyber threat management
  - User awareness
  - Security event monitoring
  - SIEM Use cases
  - Malware detection and mitigation
  - Data loss detection/prevention
  - Vulnerability management and patch management

- Resilient
  - Disaster recovery planning
  - Forensic capabilities
  - Malware analysis capabilities
  - Distributed Denial of Service (DDoS) mitigation
  - Cyber security simulation
  - Incident response
Approach 2 – Themed audits - Developing the audit plan

Leverage a cyber security controls framework to identify in scope controls and test procedures

<table>
<thead>
<tr>
<th>Risk</th>
<th>Control activity</th>
<th>NSI</th>
<th>NST</th>
<th>NIST</th>
<th>IBO</th>
<th>Cobi</th>
<th>Framework reference</th>
<th>Test procedures &amp; questions</th>
</tr>
</thead>
</table>
| Lack of a centralized or enterprise-wide information security program may result in a significant decrease in corporate culture towards cyber security which ultimately impacts how the CLIENT’s ability to respond to security incidents and the timeliness of such response. | <CLIENT> lines established an enterprise-wide cyber security framework policy, with supporting procedures in place that set forth how the CLIENT will identify and manage its cyber security risks. |     | X   |      |     |      | CSFR 3.1            | 1) Determine whether an enterprise-wide cyber security framework policy and supporting procedures have been established  
2) Identify the role group who has been assigned ownership of maintaining and updating the framework  
3) Describe the process for reviewing and updating the cyber security framework  
4) Describe how cyber security policies and procedures are communicated to employees |
| Lack of adequate investment in cyber security initiatives and technology may leave the CLIENT’s confidential information vulnerable to cyber threats. | Senior management provides adequate funding and sufficient resources to support the implementation of the CLIENT’s cyber security framework policy. |     | X   |      |     |      | CSFR 3.22           | 1) Determine whether the cyber security program have a dedicated and approved budget  
2) Describe how the budget is allocated to various resources such as technology, training, staffing, etc.  
3) Describe the frequency of budget reviews and allocation  
4) Describe the information used as input for funding review decisions |
| Without adequate involvement from the Board, the CLIENT will not be able to implement other cyber security policies across the enterprise. Further, cyber security processes will be evaluated as separate business functions making the CLIENT vulnerable to cyber threats. | The Board, or a committee of the Board, is engaged on a regular basis to review and discuss the implementation of the CLIENT’s cyber security framework policy and roadmap, including the adequacy of existing mitigation controls. |     | X   |      |     |      | CSFR 3.24           | 1) Determine how frequently the cyber security framework and roadmap is reviewed  
2) Identify the members of the committee or board responsible for reviewing and approving the cyber security framework roadmap  
3) Describe the information used as input for review decisions. These may include internal and external cyber security assessments and audits, risk management processes, etc. |
| Lack of alignment of other business processes with respect to information security may result in the CLIENT’s inability to respond to an incident in a timely and appropriate manner as guidance provided in the documentation may not be current. | A cyber security strategy that is aligned to the overall business strategy has been established. |     | X   |      |     |      | CSFR 3.85           | 1) Determine whether the overall business strategy has been considered in developing the cyber security strategy. What input has been incorporated?  
2) Describe how cyber security framework aligns with the business strategy  
3) Describe how the cyber security strategy was developed  
4) Describe the prioritization of cyber security initiatives  
5) Describe the cyber security strategy and its implementation framework |
| Without a roadmap, the CLIENT will not be able to prioritize remediation efforts and justify security budgets based on the risk exposure to the organization from potential threats. This may lead to deployment and enhancements done on an ad hoc basis without actually reducing the organization’s risk exposure. Further, without the formal cyber security roadmap, the CLIENT may also not be able to communicate security initiatives. | A cyber security roadmap has been developed that outlines key initiatives and timelines. |     | X   |      |     |      | CSFR 3.57           | 1) Determine whether a cyber security roadmap has been developed  
2) Determine the rationale based on which the roadmap timeline has been established  
3) Describe how the roadmap aligns with the overall business strategy  
4) Describe the key initiatives and their timelines |
Deloitte contacts

**David Nowak**
Senior Manager
Cyber Risk Services
Deloitte & Touche, LLP
312.486.4126
danowak@deloitte.com

**Shari Gribbin**
Senior manager
Regulatory & Compliance
Deloitte & Touche, LLP
202-207-6465
sgribbin@deloitte.com

**Amy Fread**
Manager
Internal Audit
Deloitte & Touche, LLP
713-982-3760
afread@deloitte.com