HEIN
AUDIT | TAX | ADVISORY

Hein & Associates LLP
1999 Broadway, Suite 4000
Denver, Colorado 80202

www.heincpa.com
p 303.298.9600
f 303.298.8118

Thursday, June 16, 2016

John Doe
XYZ Company & Associates

Dear Mr. John Doe:

Thank you for completing Hein & Associate's Cyber Security Assessment Questionnaire. We created this survey to help assess your level of cyber security and measure current systems against that ideal. Hein provides this educational tool to help you understand what your businesses expects from its cyber security function and to assess how your current system meets (or fails to meet) those expectations. The results deliver a great starting point for discussions among staff, executives and board members about the organization's current state of cyber security and the organization's tolerance for risk in this area.

Cyber security is not just an information technology (IT) department issue, it's an enterprise-wide issue. In most companies, IT supports the systems and functionality needed by users generate and preserve business proprietary information. As part of this responsibility, IT provides the functionality to preserve the integrity, confidentiality, and availability of digital information for all aspects of your business. However, without the combined efforts of people, process, and technology across the entire enterprise, there's only so much IT can do to address cyber security threats.

We hope the information in this assessment helps your organization better understand cyber security risk. If you would like more information, or if you need additional resources that can help your organization understand your unique environment, please feel free to contact our National Cyber Risk Team via email at consulting@heincpa.com. You may also visit our website at www.heincpa.com/security.

The Methodology

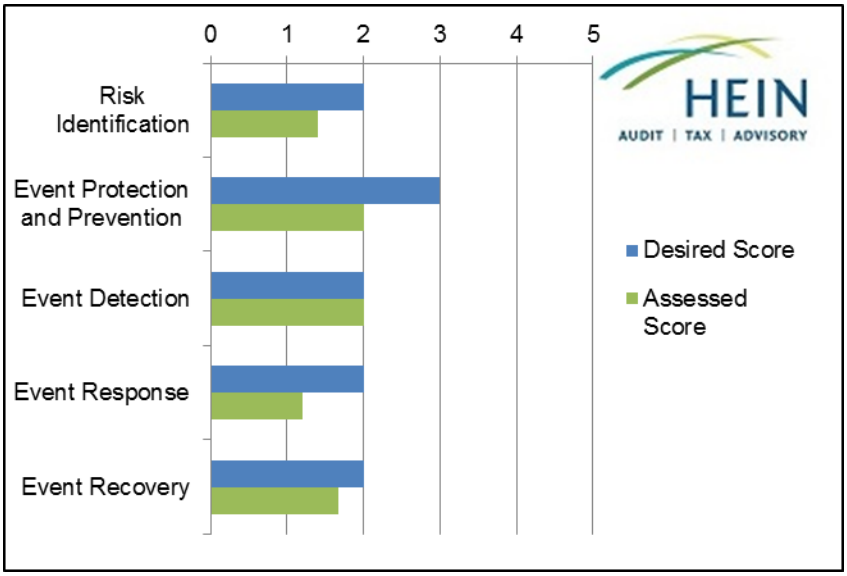
The questions in this survey were designed to identify and measure any gaps between how you believe your organization *should* perform and how it currently *does* perform in five key functional process areas of cyber security. These areas included:

- *Risk Identification:* Tools, strategies, and techniques for the identification and tracking of potential risks, and the organization's willingness to accept cyber security risk.
- *Event Protection and Prevention:* Tools, strategies, and techniques used to safeguard and ensure delivery of critical information technology infrastructures and systems.
- *Event Detection:* Tools, strategies, and techniques used to detect potential and actual occurrences of a cyber security event taking place, or an event that has taken place.
- *Event Response:* Plans and actions taken in response to an identified cyber security event.
- *Event Recovery:* Plans and actions taken for the resilience and restoration of capabilities or services impaired by a cyber security event.

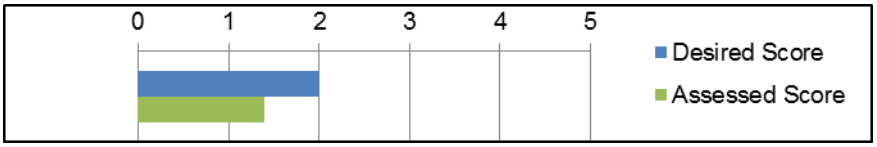
The Results

Through the results of this survey, we identified gaps between your desired and assessed score within the five key functional process areas of cyber security. The following table outlines these gaps. Please contact Hein's Cyber Risk group to investigate the potential severity of these gaps.

Table 1:

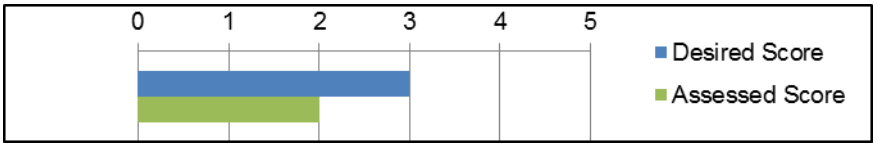


Risk Identification



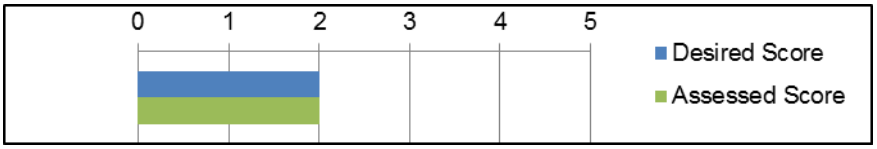
The Risk Identification function contains the basic ground work for understanding and managing cyber security risk to assets, data, and systems capabilities. By having a high score in Risk Identification, your cyber security efforts have a cyber security risk strategy in place with measurable goals tailored to your business and industry. With a score of one in the Risk Identification function, the organization may address cyber security risk assessment and strategy in an informal, ad hoc manner. The organization may not be prepared to meet regulatory requirements. The organization may not collaborate with third party stakeholders, vendors, and outsourced entities to identify and mitigate cyber security risks.

Event Protection and Prevention



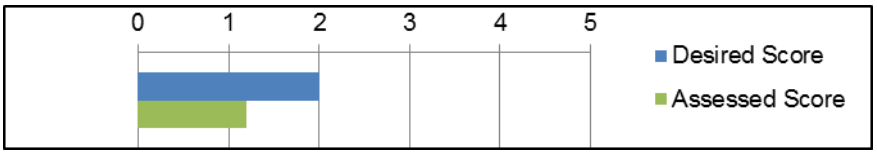
The Event Protection and Prevention function is focused on helping the organization develop and implement safeguards to reduce the impact of a potential cyber security event. By having a high score in Event Protection and Prevention, the organization may have multiple layers of cyber security defense in the form of technologies, people and procedures in place. With a score of two in the Event Protection and Prevention function, the organization may have minimal, informal, or ad hoc cyber security threat protection and prevention measures in place. However, these protection and prevention measures may not consistently work as designed, maintained, or reviewed for effectiveness. The organization may not be prepared to meet regulatory requirements. The organization may not collaborate with third party stakeholders, vendors, and outsourced entities on protection and prevention measures.

Event Detection



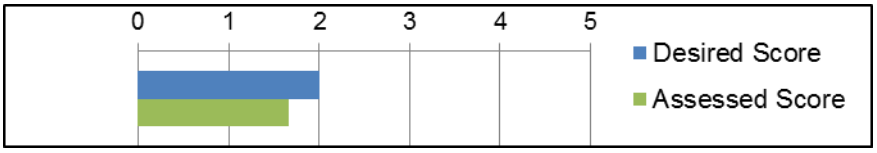
The Event Protection and Prevention function is focused on assisting the organization develop and implement safeguards to detect when a cyber security threat is present. By detecting cyber security events in a timely manner, the organization can reduce the potential impact the threat can have on the organization. With a score of two in the Event Detection function, the organization may have informal, ad hoc, and inconsistent cyber threat and event detection processes in place. As a result, the organization may not be able to adequately or consistently detect a cyber security threat or event, or may not detect the threat or event until after the event has occurred and has directly, or indirectly impacted the organization. The organization may not be prepared to meet regulatory requirements. The organization may not collaborate with third party stakeholders, vendors, and outsourced entities on detecting cyber security threats and events.

Event Response



The Event Response function is focused on ensuring that a response plan is defined and that the organization will be prepared to take the correct actions for when a cyber security event is detected or reported. By having a high score in Event Response, the organization will have a process to respond to all types of cyber security incidents with varying levels of impact. With a score of one in the Event Response function, the organization may respond to cyber security incidents in an informal, ad hoc, or reactive manner. Stakeholder roles and responsibilities in incident response may not be formalized and documented. The organization may not be prepared to meet regulatory requirements. The organization may not collaborate with third party stakeholders, vendors, and outsourced entities when responding to cyber security threats and events.

Event Recovery



The Event Recovery function is focused on what recovery actions should be taken during and after a cyber security event. With a high score in Event Recovery, the organization has a robust process for recovering from various types of service outages in a timely manner. This Event Recovery plan would include the required language for external communication that would satisfy regulatory requirements. With a score of one in the Event Recovery function, the organization may react to service outages in an informal, ad hoc manner which may result in unnecessarily long recovery times and potentially high risk impacts. Stakeholder roles and responsibilities in incident response may not be formalized and documented. The organization may not be prepared to meet regulatory requirements. The organization may not collaborate with third party stakeholders, vendors, and outsourced entities when responding to cyber security threats and events.

About Hein & Associates

The Hein Cyber Risk team helps your company assess and understand the current state of its cyber security risk. We understand that managing this involves much more than just implementing technology. It also takes the right strategies, people, and processes to address the current threat. At Hein, we help companies assess cyber risk, implement and maintain prevention and monitoring systems, continually assess risk indicators, and address cyber security threats. Our teams:

- Enhance the utilization, effectiveness, and efficiency of your available resources.
- Perform vulnerability and penetration assessments.
- Supplement your enterprise's current IT security staff to provide specialized skillsets.
- Generate innovative solutions to your company's security issues.
- Help your IT team strengthen your organization's solutions by using industry best practices.
- Implement and tune the cyber security technologies your organization has purchased, but cannot find time to implement.
- Work closely with your enterprise to manage the cyber security function.
- Audit your organization's functions and systems to evaluate the effectiveness of your security strategy, tactics, and programs.
- Maximize your enterprise's return on investment in cyber security technologies and resources.
- Develop effective incident response plans to potential security breach scenarios.
- Assess the risks of sharing information with external third parties and cloud solution providers.

At Hein & Associates, we have the knowledge, skills, and experience to help your organization assess and manage cyber security related issues. We have helped many organizations develop a strategic tolerance for information security and cyber security risks. Also, our team works hard to compliment the many skilled individuals you already have in your organization. With Hein & Associates, cyber risk mitigation is our specialty.

Appendix A – Answers and comments provided in the Questionnaire:

Part 1: How well do you feel your organization should align with the following statements:
Q: The organization understands and manages cyber security risk to systems, assets, data, and capabilities to meet its cyber security risk management strategy and business needs.
A: Disagree

Q: The organization develops and implements appropriate safeguards to protect, limit, or contain the impact of a potential cyber security event on critical information system and services.
A: Agree

Q: The organization develops and implements appropriate safeguards to identify and detect the occurrence of a potential cyber security event on critical information systems and services.
A: Disagree

Q: The organization develops and implements appropriate procedures and activities to take action, contain, and minimize the impacts of a detected cyber security event.
A: Disagree

Q: The organization develops and implements the appropriate activities to maintain plans for resilience and timely restoration and recovery of normal operational capabilities and services that were impaired due to a cyber security event.
A: Disagree

Part 2: How well do you feel your organization DOES ALIGN with the following statement:
Question #1
Q: The physical devices, software, data flows, and external information systems have been mapped, inventoried, and prioritized.
A: Disagree
Comment:

Question #2
Q: The organization's objectives, role within the supply chain, and critical infrastructure have been established and communicated to the appropriate third parties.
A: Strongly Disagree
Comment:

Question #3
Q: An Information Security Policy has been drafted that defines roles, responsibilities, and regulatory requirements.
A: Disagree
Comment:

Question #4
Q: A process has been defined for handling threats, vulnerabilities, and potential impacts to the business.
A: Strongly Disagree
Comment:

Question #5
Q: A risk tolerance and risk management process have been defined and agreed upon by stakeholders.
A: Strongly Disagree
Comment:

Question #6
Q: Credentials are managed and access permission limited using separation of duties and least privilege methods.
A: Strongly Disagree
Comment:

Question #7
Q: There is a training that takes place that educates users of their roles and responsibilities based on their role in the organization and system access level.
A: Agree
Comment:

Question #8
Q: There are adequate capabilities to protect data (data encryption, asset retirement process, redundancy, border protection, integrity checking, separate test environments).
A: Disagree
Comment:

Question #9
Q: The processes and procedures for protecting data have been defined (baseline configurations, System Development Life Cycle, change control, backups, physical protection).
A: Disagree
Comment:

Question #10
Q: Physical maintenance of assets is limited to authorized personnel.
A: Agree
Comment:

Question #11
Q: The use of removable media and the access to systems is limited or controlled.
A: Strongly Disagree
Comment:

Question #12
Q: Intrusion detection or prevention capabilities exist in the environment. Results are analyzed and prioritized based on impact.
A: Disagree
Comment:

Question #13
Q: Malicious or unauthorized code and software be can detected and alerts are monitored (e.g. logs or alerts for the network, physical environment, personnel and service provider activity are reviewed).

A: Agree
Comment:

Question #14
Q: A cyber security incident detection process is defined and tested.
A: Strongly Disagree
Comment:

Question #15
Q: A cyber security incident response plan is defined and covers high risk scenarios for your company.
A: Strongly Disagree
Comment:

Question #16
Q: A cyber security incident response plan defines internal stakeholder, and external entity, communication roles and responsibilities.
A: Strongly Disagree
Comment:

Question #17
Q: Response procedures have been defined to investigate, analyze, and categorize during a cyber security incident.
A: Strongly Disagree
Comment:

Question #18
Q: Response procedures have been defined to contain and mitigate losses during a cyber security incident.
A: Strongly Disagree
Comment:

Question #19
Q: Cyber security response plans are reviewed and updated on a defined frequency.
A: Disagree
Comment:

Question #20
Q: A cyber security incident recovery plan is defined and covers high risk scenarios for your company.
A: Disagree
Comment:

Question #21
Q: Cyber security recovery plans are reviewed and updated on a defined frequency.
A: Disagree
Comment:

Question #22
Q: A cyber security incident recovery plan defines internal stakeholder, and external entity,

communication roles and responsibilities.
A: Strongly Disagree
Comment: