White Paper

Leveraging The Power of a Cyber Risk Assessment

By Dena Cusick — Technology, Privacy, and Network Risk National Practice

Imagine you're a risk manager and your CEO asks you for an update on your company's network security position. Where would you begin and what information would you provide?

Ensuring your organization is well-protected in the area of network security and data privacy risk requires a threepronged approach: assessment, incident response, and risk transfer.

First, you need an in-depth understanding of your overall risk. That means taking the time, well in advance of the CEO's update request, to do a thorough assessment to identify the specific risks your organization faces — and the individual strengths and weaknesses of your network security plan.

Second, you need to evaluate your preparedness and your incident response plan — a documented and tested action plan that lays out every step you should take if you experience an event. What would you do if there was unauthorized access to your systems? What would you do if you had a denial of service attack, or if an employee lost a laptop? You don't want to be putting together your response plan, or testing that plan for the first time, when you're already in the middle of an event.

Third, you need to know your organization's level of risk tolerance, which brings us right back to the need for a thorough risk assessment. If you don't know how vulnerable your organization is to a cyber breach, you won't know what you need to do to address it, and you won't know how much insurance you need to buy.

Why Perform a Cyber Risk Assessment?

While most organizations have an established framework for data security, they haven't necessarily conducted a formal assessment of their organizational risk. A thorough assessment that offers well-prepared results helps you:

- Understand your risks, identify strengths and weaknesses of your network security position, and make suggestions for improvement. You can provide tangible information to senior management to help them better understand your cybersecurity strengths and weaknesses.
- Obtain the information you need to help you make informed cyber risk management decisions, with the end goal of establishing a resilient enterprise that minimizes breaches and their impacts.
- Determine whether the level of protection afforded by your current internal cybersecurity program is adequate, or whether you should consider steps to improve your position.
- Set a target state of cybersecurity preparedness that best aligns with your organization's risk appetite, and determine how much risk you want to transfer to an insurance program.
- Provide concrete assessment results that your insurance broker can use to negotiate the best insurance premium, coverage enhancements, and deductibles on your behalf. Terms and conditions tend to be highly subjective in the cyber insurance industry, and an assessment that highlights your strengths can help your organization get more favorable pricing and terms and conditions from the underwriter.
- Address the financial and cultural impact that making the suggested changes can have. It is important to strike a balance between network security and your employees' ability to function and do what they need to do on the job.
- Decide how and where to allocate your budget for network security. Your results may also help you secure budgets for certain resources in specific areas of the organization

Another key advantage of an assessment is that it helps create a defensible position in case of a breach. After a breach, the first step is often a request for the date of your last cyber risk assessment, along with a copy of your incident response plan, information on when the plan was last tested, and any employee awareness training you have implemented.

These requests may come from a plaintiff's attorney, a payment card provider, a state attorney general, or, in the case of a healthcare data breach, the federal government's Office for Civil Rights.

Third-Party Assessments: Value and Considerations

One of the crucial ways that an organization can assess its risk related to data is through a third-party assessment. This is advantageous because it provides an objective perspective. The assessment may include questions you never thought to ask, which can help you identify risks that you weren't even aware existed. Considerations for a thirdparty assessment include:

Scope

Third-party assessments can range from a comprehensive on-site evaluation by a consultant to a brief questionnaire. Many organizations settle on a solution somewhere in the middle of this spectrum, such as a web-based cyber risk management tool.

Stakeholder Inclusion

Ideally, the assessment tool will bring multiple stakeholders together to provide a picture of your organization's position. This allows people to answer the specific questions that fall within their areas of expertise.

Depending on your organizational structure, key stakeholders might include your risk manager and heads of security, compliance, human resources, technology, legal, and procurement or vendor management. Everyone's time on the front end will yield valuable results on the back end.

Standards to Assess Risk

There are a number of standards that are used as the basis for assessing risk. The National Institute of Standards and Technology (NIST) Cybersecurity Framework is one of these standards. NIST is an agency of the U.S. Department of Commerce that develops measurements and standards for cybersecurity.

> *"[The NIST framework] will help companies prove to themselves and their stakeholders that good cybersecurity is good business."*
>
> — NIST Director Patrick D. Gallagher in a news release1 announcing the launch of the framework

The NIST framework is based on five functions — identify, protect, detect, respond, and recover. Taken together, these allow an organization to understand and shape its cybersecurity position.

- **Identify**: understanding the business context, the resources that support critical functions, and related cybersecurity risks allow an organization to focus and prioritize its efforts
- **Protect**: ability to limit or contain the impact of a potential cybersecurity event
- **Detect**: timely discovery of cybersecurity events
- **Respond**: take action and contain the impact of a potential cybersecurity event
- **Recover**: timely recovery to normal operations to reduce the impact of a cybersecurity event[2]

How can we help?

Besides negotiating the most favorable terms and conditions with carriers, USI Insurance Services offers access to other value-added services from certain insurance carriers, such as:

- A simulated phishing email attack, which allows you to track those employees who click on a phishing link in an email, and then offer them additional training
- Guidance and assistance with managing your compliance to applicable standards, such as payment card industry and Health Insurance Portability and Accountability Act (HIPPA) requirements
- Training designed to continue to evolve your organization's cyber risk awareness

For more information regarding this topic, please contact your USI consultant, or visit us at www.usi.com.

Sources:

1. National Institute of Standards and Technology news release
http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm
2. NIST cyberframework
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf