NAVIGATING CYBER RISK

by Steve (Ryan) R. Corbin, VTS Software Engineer

Cyber criminals strike again! Your peers, partners, competition, or maybe even you have personally become a victim of cyber crime. You realize you're at risk, but what can you do about it? Cybersecurity is a massive topic and there are a plethora of tools claiming to help companies secure their digital footprint. However, resources are finite and very few companies can afford a shotgun approach to securing their systems. Cybersecurity is a continuously evolving process that requires short and long-term planning. You can think of cybersecurity like an epic journey. You have to know where you're starting from, where you need to go, how you will travel, and how to make sure you are staying on track.

WHERE ARE WE GOING?

Critical Systems and Information

The first step is to determine what needs to be protected. This will assist in establishing an organization's security goals and objectives. Setting security and privacy objectives involves identifying the critical systems and information that need protection. This could be proprietary information, financial information, customer and employee personal information, system credentials, business systems, or any other data or system often targeted by cyber criminals. NIST IR 8179 [1] lays out a process for determining the criticality of systems and components. The process involves identifying the critical activities, systems, and system components for each program, and analyzing the results to prioritize them. Critical systems often include third party services used in business processes such as payment processing, Human Resource services, web hosting, and more.

Once the critical systems and information have been identified and prioritized, the organization can begin identifying security goals and objectives. An organization's security goals and objectives should align with their business goals and objectives, while focusing on the critical systems and information that have been identified. This allows an organization to develop an informed investment strategy for cybersecurity that protects critical infrastructure supporting their business priorities.

WHERE'S THE STARTING LINE?

Risk Assessment

You can't figure out which direction to go if you don't know where you are. For cybersecurity that means knowing your risk. Cyber risk is a function of the adverse impact of a threat occurring and the likelihood that it will occur. [2] An organization can get an idea of the initial risk to a system or business process by conducting risk assessments targeted toward critical systems and information. While a risk assessment is not a precise measure of risk, it is a critical process that reveals risk that exists in and between business processes and information systems.

Assessments should be based on risk models and bound to a particular time frame. Risk models explicitly define risk factors and their relationships to be assessed. Models should contain threats,

[1] https://csrc.nist.gov/publications/detail/nistir/8179/final
[2] https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
Steve (Ryan) R. Corbin - rcorbin@vtscyber.com
703.498.2150 703.498.2149

events, vulnerabilities, impacts, likelihood of events occurring, and predisposing conditions. Threats from purposeful attacks, environment disruptions, human errors, machine errors, and structural failures can be coupled with threat sources and vulnerabilities to create threat scenarios. Organizations should consider how threat sources will adapt their attacks to security measures on the system. Likelihood should be determined by considering the probability that a threat scenario or event will be initiated and the probability that it will have an impact on the system or business.

Assessments can be quantitative, semi-quantitative, or qualitative. Quantitative assessments allow for improved cost/benefit analysis and support repeatability, but require more effort, tools, and expertise to create. Qualitative assessments are easier to perform and understand, but are less useful when prioritizing and comparing risk response. Semi-quantitative assessments require expertise, but provide an easy to understand result that allows for comparing and prioritizing risk response and courses of action.

Risk assessments can be analyzed in a threat-oriented, vulnerability-oriented, or impact-oriented approach. Threat-oriented analysis will begin with the threat and focus on threat scenarios, how threats exploit vulnerabilities, and what impacts are expected based on the threat sources intent. A vulnerability-oriented approach focuses on vulnerabilities and predisposing conditions and identifies which threat sources and events are capable of exploiting the vulnerability. This can help account for multiple events or impacts expected over the specified time frame. An impact-oriented approach will focus on impacts to specific assets and identify the threat events, sources, or scenarios that could produce a consequence of concern.

Risk assessments facilitate decision making at all levels, and should be performed frequently to maintain the specific knowledge of what is at risk. NIST SP 800-30 [3] provides more information about how to conduct effective risk assessments.

PLANE, TRAIN, ROCKETSHIP?
Security and Privacy Controls

Now that we know where we are starting, which way to go, and where we need to end up, we can begin to plan how we are getting there. This means how we are going to respond to the risk. We must develop and evaluate possible courses of actions and determine the appropriate action to take. The appropriate action is going to mitigate risk, and for cyber risk that is going to involve selecting and implementing security and privacy controls.

Controls are not limited to software and technology solutions. Training, policies, and other business functions can also control security and privacy risk. Security controls are safeguards and countermeasures employed to protect information systems and the data stored on them. These controls are selected based on regulatory compliance requirements and the analysis of results from risk assessments or continuous monitoring. Privacy controls are safeguards employed to protect personally identifiable information (PII), and are often required for regulatory compliance.

[3] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
Steve (Ryan) R. Corbin - rcorbin@vtscyber.com
703.498.2150 703.498.2149

NIST identifies three types of control implementation approaches, common controls, system-specific controls, and hybrid controls. Common controls are controls that are inherited across multiple systems. This is a cost effective approach, but a common control may not provide the same level of protection across a system. System-specific controls provide the exact level of protection for each system, but are not cost effective and require more work to maintain. A hybrid system uses common controls to provide basic security across all systems, and implements system-specific controls to provide additional protections needed. The hybrid method is the most cost-effective method for selecting controls to protect an organization's systems.

Improperly identifying what system-specific controls are needed can easily change a hybrid approach into a system-specific approach, by selecting unnecessary system-specific controls. System-specific controls should be selected to meet the goals and objectives identified previously and be trustworthy. Trustworthy controls are controls that are or will perform as expected and provide all of the features and functions needed.

NIST SP 800-53 [4] provides more information about security controls, and includes a 357 page catalog of controls with in-depth information and references for each. NIST SP 800-53B [5] describes the baseline controls for a system based on its impact level. Instructions for determining a systems impact level and establishing minimum requirements for federal information systems can be found in FIPS 200. [6]

DIDN'T WE JUST PASS THAT TREE?
Measuring Controls

The trustworthiness of a control depends on the control performing as expected, but waiting for an attack to find out is a bad strategy. Controls should be measured and risk continuously monitored. NIST SP 800-55 [7] provides guidance for developing and implementing measurements for cybersecurity controls.

When measuring controls, it is important to remember that measures must be quantifiable (numbers based), easily obtainable, useful for directing resources, and repeatable. Measures should also focus on three areas, implementation, effectiveness and efficiency, and impact.

Implementation measures can be fairly easy to measure using percentages. Percentages of people, systems, and practices where controls are implemented can be easily measured. An example would be what percentage of the work force has had cybersecurity training each year. This is useful information quantified with a percentage, easily obtained through HR or automated training records, and repeatable each year.

Effectiveness and efficiency measures require more skill and expertise to develop. These measures provide insight into the results of security controls. Effectiveness measures will measure how robust the security controls are, while efficiency measures gauge the timeliness of the results. An example for this is

4 https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
5 https://csrc.nist.gov/publications/detail/sp/800-53b/final
6 FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (nist.gov)
7 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
Steve (Ryan) R. Corbin - rcorbin@vtscyber.com
703.498.2150 703.498.2149

the percentage of available security patches installed at a certain time. This demonstrates how effective your update procedures are, as well as how efficiently they are being applied. This information allows businesses to determine if their IT team is properly staffed and equipped to keep up with the number of security patches being released. It can also reveal buggy software that should be replaced with more stable and secure options.

Impact measures are used to measure the impact the information system is having on the overall organization. This will provide the most direct insight for how the security controls are impacting the organization. This type of measure should be carefully selected to ensure that the benefit is properly measured. Measuring the cost of security controls across different programs and departments is important, but a well run security program will have to be measured against the potential risk along with the cost of responding to security events that have occurred. It can be easy to see the security program as a drain on the budget, if you are not implementing controls to detect and report when attacks fail and recognizing that some attempts will go undetected if deterred early enough.

Measuring controls provides an organization with the ability to monitor its risk. Assessments, reports on security metrics, critical systems, security goals, and security objectives should all be updated periodically. Cyber threats are constantly iterating and improving on their designs, and cybersecurity programs must do the same. These reassessments should identify risk-impacting changes to the system or environment, and verify that planned responses are being implemented and that they are in line with business functions and external obligations.

The final destination for Cybersecurity is like a point in the middle of the ocean. It requires continuous monitoring and course correction because there is no way to anchor to it. Waves of Cyber criminals, updates, and vulnerabilities will constantly push an organization off of its spot, and require some sort of effort to bring it back. Risk assessments, controls, and measurements are three of the most important actions a business can take to keep their ship from going aground.

14900 Conference Center Dr,
Suite 200
Chantilly, Virginia 20151

info@vtscyber.com
Steve (Ryan) R. Corbin - rcorbin@vtscyber.com
703.498.2150 703.498.2149