INTERACTIVE SECURITY

COMPLETING A YEARLY RISK ASSESSMENT: *A best practice for protecting IT systems against everchanging and costly cyber threats*

Yearly assessments are necessary because no organization in the 21st century can afford for IT systems to face compromise without a plan of defense, response, and recovery.

Author: Emory Vandiver
VP Business Operations/Partner
Interactive Security
www.intactsec.com
267.824.2500

For some organizations, yearly reports are an exercise in box checking. Leadership wants reports, but rarely examines them or uses them for implementation. Staff sees the compilation of the assessment in terms of going through the motions to satisfy the higher-ups. Most institutions and organizations engage in this at some level, but IT yearly risk assessments should always be done and always be taken seriously.

An IT risk assessment is an assessment of threats to an organization's IT system. It starts with a business (or organization) impact analysis, also referred to as a BIA. The BIA analyzes a business or organization's most crucial processes. One of the most important sections of a BIA lies in the description of threats to crucial processes, the potential impact of threats, and recovery, which naturally leads into an IT risk assessment.

The IT risk assessment specifically addresses potential threats to the IT system of an organization. Most people logically think first of cyber attacks, data security, and other issues since these potential problems dominate news coverage. Disruption of IT, however, could also come from natural disasters, fires, equipment malfunction, and other issues.

The Importance of the Yearly Risk Assessment

Very few threats to an organization remain static. Crime rates go up or down. Weather patterns often change substantially from year to year no matter what people believe causes them. Government regulations and their impact change. No threat, however, changes more often, more drastically, or potentially more destructively than threats to IT systems.

Any organization's yearly risk assessment should include identifying threats and vulnerabilities, potential man-made and natural hazards, defensive responses, impacts of threats, and the recovery process. Every aspect of the yearly risk assessment requires review annually, not just the cybersecurity aspect. Most people understand that risks from online, as well as response and recovery, change all the time. IT risk and recovery from other fields can change as well. For example, weather or earthquake forecasting and modeling can improve, which would give an organization more time to put emergency protective measures in place.

Yearly assessments are necessary because no organization in the 21st century can afford for IT systems to face compromise without a plan of defense, response, and recovery.

Who Should Do a Yearly Risk Assessment?

Some organizations have higher profiles that serve as magnets for attention and attack. These include national political parties, state election offices, major companies, and controversial political organizations. Obviously, these organizations should do yearly or more frequent assessments. Not so obvious are other organizations. In recent years, local school systems, senior service organizations, and other similar groups have undergone attacks from malefactors seeking to gain personal information illicitly.

Additionally, threats to systems can come from flood, fire, earthquakes, and severe storms. In other words, every organization that relies heavily on their IT system needs an effective yearly (or more) risk assessment.

Knowing Your Risks

Identifying risks starts with an examination of the threats to organizational processes in the BIA. Threat information can come from a wide variety of sources. These include:

- Company history of threats and responses
- National Weather Service, NOAA, FEMA, US Geological Survey, and other government sources to ascertain natural disaster threats. For example, everyone knows California suffers severe earthquakes, but fewer understand the history of catastrophic events in Missouri
- Key stakeholder organizations
- Regional and state history sources, including academics if available
- The US Department of Commerce's Information Technology Laboratory offers more information on identifying risks

Next, the assessment should acknowledge and describe the two major categories of risk, man-made and natural. Man-made hazards come from deliberate or even accidental threats to IT from one or more people. Accidents should receive attention alongside intentional attacks on the system. These can come from employees misusing technology to even breakages of equipment. Natural hazards come from what are officially referred to as "Acts of God" for which no one can be held responsible.

After identifying the range of risks, a good risk assessment should then examine the impacts that could occur if the threats materialize. These include:

- denial of access
- data loss
- loss of personnel
- loss of function
- lack of information

A risk assessment will certainly include many of the "nuts and bolts" of physical and cyber recovery from the impact of a materialized threat. This will include the replacement of equipment, re-establishment of programs and operations, and other important recovery issues. It should also include analysis of recovery from secondary consequences. For a business, this will usually center on re-establishing and rebuilding the customer relationship as quickly as possible. Both businesses and other organizations depend on reliability and trust from customers or other types of clients. Rebuilding the brand and relationships of trust, if the threat harmed those, is essential to recovery.

Financial impact and recovery also represent essential areas that an organization must address. What could it cost to restore the system and service? How much will insurance cover?

These represent two examples of medium and even possibly long-term risks to the organization after the onset of a problem or disaster that affects IT.

Yearly Changes Open New Risks

Threats never remain the same or else organizations would find them easy to counter. Some grow worse or more complex, others change their nature, and some are inherently unpredictable.

One ever-changing aspect of IT lies in something that is not an intentional threat but remains a constant factor in how to run systems, recover from disasters and man-made attacks, and respond effectively afterward. Government regulations, other legal protocols, and the possibility of liability always change. Just in the past few years, both US and European Union agencies have introduced new protocols governing data security. Lack of adherence could have serious impacts on a business if data is compromised during an attack.

Data thieves grow ever bolder and more sophisticated. They have preyed on the naivete of organization employees in the past in sending malware through official email, but they are getting better at identifying and attacking vulnerable systems. Data thieves do not care if they steal personal information from Citibank or Rural County Senior Services; they will attack the path of most efficiency and least resistance. Every organization with something to protect should annually assess their risk.

Other sophisticated attacks come from foreign government and nongovernment sources, such as terrorists or radical activists seeking to score political points. They seek to steal secure and potentially embarrassing information or shut down a system in a manner designed to create ridicule. As they tangle with the federal government and the cybersecurity community, like dangerous bacteria, the ones that survive grow more resistant to preventative measures. No one can count solely on preventative and protective measures anymore. Response and recovery planning is essential in a yearly assessment.

Experts said before World War II that “the bomber will always get through.” Almost a hundred years later, one can say, “the hacker will always get through.” The job of a yearly risk assessment is to ascertain how to prevent, and if that is impossible, minimize or mitigate the damage. Organizations that either fail to perform a yearly risk assessment or fail to take the threats seriously set themselves up to fail and put their customers and/or clients at risk.

About Interactive Security

Since 2007 Interactive Security, Inc. has been at the forefront of providing industry leading expert information technology security services to clients across the globe - focused on IT Security Auditing & Compliance.

Our team is comprised of highly skilled industry certified professionals with diverse experience serving technology consulting firms and enterprise security departments. We serve a broad base of clients and industries including the payment card industry, finance, legal, healthcare, education, government, restaurant and hospitality.

Our clients and partners choose Interactive Security because of our uncommon ability to provide expert custom IT security services that exceed both technical and business expectations.

*We pride ourselves on Making **IT COMPLIANCE OBTAINABLE, SIMPLE AND AFFORDABLE.***

*Vulnerability / Penetration Assessments * Application Security * BCP/DR Planning * PCI DSS * HIPAA * HiTRUST * ISO 27001-27002 * ISO 31000 * NACHA ACH * FEDRAMP * FISMA/NIST * GDPR * Privacy Shield*