Guidacent®

Guidacent Special Business Brief

The Four A's of Cybersecurity

For Business Operations

Guidacent®

The Four A's of Cybersecurity
For Any Business Operations

risk ♦ *(cybersecurity)*

1. exposure to harm or loss resulting from breaches of or attacks on information systems.

2. results extend beyond damage and destruction of data or monetary loss and encompasses theft of intellectual property, productivity losses, and reputational harm.

Managing Risk. That's a tall order for financial institutions of all sizes and across the nation. Organizations that are trying to keep ahead of their competition while also trying to defend those critical assets are continuing to fall behind in the fight

Simply stated, Cybersecurity risk refers to the potential of loss or harm related to technical infrastructure or the use of technology within all businesses that rely on information technology as part of their core operations.

Ransomware has plagued businesses for several years now. Successful attacks have caused companies to lose millions of dollars in ransom payments, encouraging hackers to keep using and refining these attacks.

Recent cybersecurity reports reveal that the process by which attackers are able to purchase ransomware kits on the dark-web is becoming easier. Not to mention, the ransomware itself is becoming increasingly more sophisticated.

As historical evidence (and the news), continue to validate, no business operation is safe from compromise. All business activities carry an element of risk, and many organizations are far less prepared for a compromise than what they may think.

Managing and mitigating risk is the responsibility of everyone in throughout the organization. But managing risk may be far less challenging when we understand what those risks are and where (and how) they are most likely to originate.

Defining ***Risk*** and identifying how it impacts a financial institution can take on many different shapes and sizes.

Businesses are becoming more vulnerable to cyber threats due to the increasing reliance on distributed and remote computing environments, programs, and social media.

It's also no longer enough to remain dependent upon traditional reviews and compliance guidelines as defined by PCI, SOX, GLBA and the emergence of the GDPR and CCPA.

Moreover, institutions often face the paradox between paying for tools that seldom get deployed properly and hiring security people who may not be fully aware or qualified to address what's in the wild.

Why it Matters

- $6 **trillion** in estimated losses (2021) from cybercrime
- 90% companies admitted to protected data being exposed or **compromised**
- 79% firms consider *Risk Management* a Top 5 **Priority**

FBI

Cybersecurity risks also extend beyond damage and destruction of data or monetary impact. The loss of intellectual property, productivity, and reputation are often further collateral damage resulting from a compromise and can follow an institution out to every branch in the system.

Some risks are technical, like a component that might turn out to be difficult to use, while other risks are external (i.e., changes in the market or even problems with the weather). Managing risk also means often balancing between what is expected and what is *tolerated*.

Complicating this equation is the emergence of cyber as one of the most impactful sources of risk in the modern enterprise. In fact, *cybersecurity* is now increasingly scrutinized by corporate boards and state and federal auditors and often extended out to include financial analysts, who see cyber security risk as an imminent and existential business and financial risk.

No matter how well we plan, our projects and the infrastructures we manage, the operation is still likely to encounter unexpected problems. Two factors come to light:

1. Understanding how much risk a business owner is willing to tolerate;

2. Thinking about how much the operation is willing to invest or spend to manage risks that are either known or anticipated (i.e., internal, unintentional, external, etc.).

Internal risks, for example, stem from the actions of employees inside the branch or main office (i.e., malicious systems sabotage, data theft by a disgruntled employee).

An example of unintended, internal risk, by contrast, may include an employee who failed to install a security patch on out-of-date software.

When evaluating the general level of risk within an institution, there will always be a certain aspect of uncertainty. Some risks, however, do occur, which is why addressing risk is critical to any business.

Risk-centered Cybersecurity Focus

In a *risk-centered* approach to managing cybersecurity-related activities, two essential points of impact emerge as critical results from the effort:

First, the approach focuses on reducing risk as a primary objective, allowing businesses to prioritize their capital investment and corresponding resources, predicated upon cyber initiatives aligning with the ability to reduce risk.

Want to Reduce Cyber Risk?

- **Multi-factor authentication**
- **Strong, Complex Passwords**
- **System Patches & Updates**

Second, a risk-centered approach classifies key objectives into specific, measurable outcomes as directed by senior executives.

Focus remains on designing and implementing processes and controls that provide the broadest coverage, yielding the greatest impact to critical operations.

Given the many sources of cyber risk, with each event having different levels of potential impact, prioritization is critical. Determining how and where to allocate human, financial, and technology resources can be a challenge.

The formula includes both intangible and tangible assets, is subjective, and includes variables based on institutional comfort, priorities and governance, risk and compliance policies, regulatory obligations, and legal commitments.

For many organizations, establishing a resilience to risk of compromise requires more than incremental improvements. It requires focus on business risk, rather than technology controls alone.

A⁴ Risk Management Model

There are four types of risk mitigation tactics that comprise the various mitigation techniques that may be implemented as an effective means of reducing the infrastructure risk profile within any organization.

Avoiding the problem in the first place is always a good way of staying out of trouble. If you can prevent a risk from occurring or worse—metastasizing into something even more damaging.

It's in the best interest of everyone to do so.

Risk avoidance usually involves developing an alternative strategy that has a higher probability of success but usually at a higher cost associated with accomplishing a project task, but McKinsey reported that companies that try too frequently to avoid a risk result in impacting lower overall performance, thereby "squandering reasonable opportunities to grow and achieve [business] objectives."

A common risk avoidance tactic is to use proven, existing, and credible technologies rather than adopt new techniques, even though the new techniques may show promise of better performance or lower costs.

A project team may, for example, choose a vendor with a proven track record over a new vendor that is providing significant price incentives to avoid the risk of working with a new vendor.

CYBERSECURITY – To reduce the risk of compromise to critical infrastructure operations within an organization or entity.

Risk Mitigation ("Apply")

When faced with a situation that you know has risk, and you know you aren't going to be able to avoid it, *Apply* (or **mitigate**) the appropriate controls and processes you have available to address the issue to minimize risk.

Risk mitigation provides a means of capturing the risk mitigation approach for each identified risk event and the actions the project management team will take to reduce or eliminate the risk.

This means taking some sort of action that will cause it to do as little damage to your infrastructure as possible. Risk mitigation equates to preparing for and reducing the effects of threats faced by a business.

Risk mitigation takes steps to reduce the negative effects of threats and disasters on business continuity. When considering risk mitigation, activities do not need to be complicated. Something as simple as adjusting the workflow of an operation or as complex as implementing a new system application to reduce human intervention in a workflow, are examples of risk mitigation.

Risk Assignment

Risk Assignment involves partnering with others to share responsibility for the risky activities. Many organizations that work on international projects will reduce political, legal, labor, and others risk types associated with international projects by developing a joint venture with a company located in that country.

Weather, political unrest, and labor strikes are examples of events that can significantly impact the project and that are outside the control of the project team.

Partnering with another company to share the risk associated with a portion of the project is advantageous when the other company has expertise and experience the project team does not have.

The purchase of insurance is usually in areas outside the control of the project team.
If a risk event does occur, then the partnering company absorbs some or all of the negative impact of the event.

But in the world of IT management, Assigning risk more commonly equates to assigning services out to an MSSP or other security service provider or resource.
Incorporating tools such as Security Incident and Event Monitoring tools or SIEMs, firewalls, and multi-factor authentication tools deployed throughout a system, are additional methods to assign risk.

Assigning highly skilled project personnel to manage the high-risk activities is another risk-reduction method. Experts managing a high-risk activity can often predict problems and find solutions that prevent the activities from having a negative impact on the project.

The risk is transferred from the project to the insurance company. And from a cyber perspective, a common example is when a firm gets hit with a ransomware attack and has no alternative but to pay the ransom.

In such cases, smart-thinking business executives were grateful they had Cybersecurity insurance to help fray the expense, which is often north of several million dollars.

Risk Acceptance

Some risk is necessary to function in today's business environment. When you can't avoid, mitigate, or assign a risk, then you must accept its inevitability.

The objective of accepting risk often translates into continuous monitoring of those risks, and providing adjustments as needed, to the overall risk management strategy, to avoid consequences from a compromise or exploit as a result of a known risk.

But even when you accept a risk, at least you've looked at the alternatives and you know what will happen if it occurs.

Essentially, unless avoiding the risk altogether, by default, you are accepting a form of the risk (whether through mitigation or through assignment to third party).

Managing Cyber Risk

Cyber risk has the potential to affect every aspect of an organization, including its customers, employees, partners, vendors, assets, and reputation.

As such, an effective cyber risk management program involves the entire organization.

Guidacent®

Cybersecurity is at the top of the agenda today for business owners of all sizes, because the stakes have never been higher.

Innovations and strategic advances that organizations make continue to raise those stakes, and Risk management isn't a problem that can be solved by merely looking the other way. Moreover, *cyber risk* cannot be completely eradicated, but it can be managed to ease the success of a company's efforts in meeting its business objectives.

Decisions about cyber risk appetite need to be made with the business and communicated throughout the organization.

What Financial Institutions should ask NOW!

- Is the Risk **Timely**?
- Is the Risk **Relevant** to business operations?
- Is the Risk **Pervasive** & capable of spreading?
- Does this Risk pose an **Urgent** impact to the business?

Guidacent has prepared a 10-question Security Self-assessment for **Business Owners**. You can access this at

guidacent.com/CyberOps

Take the first step in reducing the risk of compromise by performing this important self-assessment!

Managing Cyber Risk goes beyond identifying who's climbing the mountain with you—it's everybody's responsibility.

For many organizations, becoming truly resilient to cyberattacks requires more than incremental improvements. It requires organizational transformation that broadens the scope of involvement at the top of the organization and instills focus on business risk, rather than technology controls. It requires the ability to focus investments on mitigating likely outcomes, based on a broad understanding of attacker motives and the ability to anticipate high-impact scenarios.

The consulting teams at Guidacent view cybersecurity and risk management as elements to better enable businesses to build strong, secure operating environments, which extends the value of our digital infrastructure and economy.

If your organization would like to explore how to evaluate and address risk and build on the integrity of your critical assets, contact us at ***cyber@guidacent.com.***

Our Threat*Recon* Security Services offer four tiers of cybersecurity consulting that are tailored to fit size, budget and level of risk.