SYSTEMS
engineering

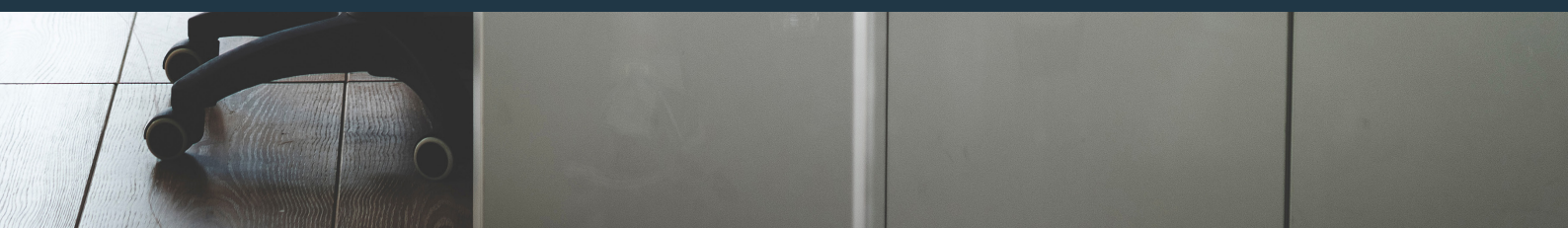
SYSTEMS ENGINEERING

CYBERSECURITY RISK ASSESSMENT

IDENTIFY AND ADDRESS RISK

INSIDE:

- PURPOSE OF AN ASSESSMENT
- ELEMENTS OF A QUALITY ASSESSMENT
- ASSESSMENT FINDINGS AND SUMMARY



INSIDE

CYBER RISKS ARE ON THE RISE

The statistics are staggering. According to Verizon's Data Breach Investigative Reports 2022,

- **the number of reported breaches among small to medium-sized businesses (SMB) has increased by 57%,**
- **the number of exposed records is up 29%, and**
- **the average cost of a data breach has hit a record high of $4.2 million.**

These numbers stress that the threat is very real…and accelerating.

Cybercrime is big business. The more industrious hackers have turned their criminal activities into full-fledged, income generating enterprises. Known as "Cybercrime-as-a-Service," this illegal business model is providing hackers with out-of-the-box cyberattack kits. This service gives even the most novice hackers access to the resources and tools they need to launch widespread cyberattacks without great investment.

The reality is no business is immune and SMBs are increasingly facing the same cyberattacks as large enterprises. In fact, cybercriminals prey on smaller companies as they tend to be less secure and, therefore, softer targets.

The statistics show that data breaches are costing organizations millions in business disruption, repair, and data loss. On top of the hard costs, the blow to their reputation can be the most significant impact. The truth is, it's hard to measure the future loss of business opportunities and revenue. When these impacts are compounded, some companies go out of business within months.

What should be noted is that a breach typically does not happen overnight. More likely, breaches happen in multiple stages, involving numerous techniques and methods. By having various protections in place, SMBs can guard against the flurry of cyberattacks that happen quietly, one small vulnerability at a time.

DO YOUR CYBER DEFENSES HOLD UP TO MODERN CYBERATTACKS?

A reliable way to know if your current cyber defense is effectively keeping the bad guys out is to perform a cybersecurity risk assessment on your environment. This comprehensive review identifies the cyber risks and gaps present in your current defense strategy. The evaluation assesses the effectiveness of your cybersecurity controls and provides clear direction on where the business needs to fortify its defenses.

In this eBook, we detail our cybersecurity risk assessment methodology that helps SMBs understand their ability to defend critical assets and identify their high-risk cyber vulnerabilities on which to **PRIORITIZE and ACT**.

Thank you for reading and making cybersecurity a business priority.

SYSTEMS engineering

1 PURPOSE OF A CYBERSECURITY RISK ASSESSMENT

WHY CONDUCT AN ASSESMENT?

As the cyberthreats evolve and your organization adopts new technologies to help your business run faster, smarter, and more efficiently, new risks will emerge that challenge your organization's ability to stay secure. Combating modern threats requires constant management coupled with an evolving security strategy that includes advanced protection measures, 24x7 detection capabilities, and periodic security assessments to ensure your business' data and systems continue to be effectively protected in a dynamic threat environment.

IDENTIFY YOUR RISKS AND ADDRESS VULNERABILITIES

As technology evolves, so do cybercriminals and their attack strategies. To combat cyberthreats, businesses need to stay on top of their methods and deploy cybersecurity measures to mitigate cyber risks.

MAKE INFORMED SECURITY DECISIONS & INVESTMENTS

When you understand the possible attack surfaces and measure the effectiveness of your defenses, your business can focus its security spend on priority items ensuring your security dollars are appropriately invested.

COMPLY WITH PARTNER OR GOVERNMENT REGULATIONS

Every industry has common, agreed-upon standards about security. To comply with them, you must start with solid information security standards, then layer in industry-specific nuances.

58%

OF SMALL TO MEDIUM-SIZED BUSINESSES WERE BREACH VICTIMS IN 2021.

Identity Theft Center's Business Aftermath Findings 2021 Report

2

ELEMENTS OF A

QUALITY CYBERSECURITY RISK ASSESSMENT

BEYOND THE TECH

An effective cybersecurity risk assessment goes beyond using tools to evaluate cybersecurity controls. It is most effective when key company stakeholders participate in interviews to discuss their standards, processes, concerns, compliance obligations, and security. Obtaining this intel helps assesors gain a better understanding of an organization's cybersecurity posture.

CYBERSECURITY CATEGORIES OF EVALUATION

SYSTEMS ENGINEERING CYBERSECURITY RISK ASSESSMENT

When conducting an assessment, Systems Engineering references several security frameworks to ensure an environment is in alignment with current security best practices and recommendations. These frameworks include NIST and ISO standards, as well as standards generally adopted across highly-regulated industries, such as banking and financial services, defense contracting, and healthcare.

GOVERNANCE, POLICIES & PROCEDURES

Creating and maintaining these critical documents helps influence your day-to-day business, providing guidelines for staff to follow when making decisions, or taking specific actions. These documents include Acceptable Use Policy, Information Security Policy, Disaster Recovery Plan, Business Continuity Plan, and other industry-specific guidelines. These documents are reviewed for their effectiveness verifying the controls you have in place and validating your staff is following set guidelines.

PERIMETER SECURITY

Your perimeter security contains multiple defenses to protect your organization. The needs in this area have changed dramatically over the last several years, and most networks are not adequately designed to defend these changes. In this category, we begin by assessing the underlying network architecture to ensure you are protected against the latest threats. We also assess the physical securities you have in place to safeguard your end-users, devices, and equipment. The proliferation of wireless networks and the integration of the Internet of Things, has made this area of defense a critical line of defense.

INTERNAL PROTECTIONS

With modern concepts such as defense in depth, it is critical to protect each component of your network. The goal is to defend against privilege escalation and other multi-stage attacks. The most significant breaches require three to five sub-attacks to bridge enough layers of defense to reach paydirt. Discovering how you keep servers patched, update antivirus signatures, monitor network events, address security alerts, and other security maintenance tasks will determine how effective your protections are. Cybercriminals are continually changing their techniques, which means the approaches you have must be maintained in order to keep them out.

SERVER & ENDPOINT MANAGEMENT

Today, about 60% of organizations allow employees to use their own devices at work, which has nearly doubled, and in some cases, tripled the number of endpoints an organization needs to manage. In this category, you'll be assessed on your business' abilities to discover, provision, deploy, update/patch, and troubleshoot all your endpoint devices. The good news is that you can now extend endpoint protections to Bring-Your-Own-Devices without major impacts to usability and productivity. This first requires an understanding of the devices that are being used and implementing technology solutions that address your specific needs.

IDENTITY MANAGEMENT

In this cloud-connected world, it is critical to identify your users, authentication them, and understand what capabilities and access they should have. Our security assessment evaluates who has access to your network, what they have access to, and how they access it. We determine whether appropriate roles and access privileges are established to control user access to critical information. We also identify opportunities to increase security while taking burdens off your end-users.

CLOUD, WEB AND EMAIL MANAGEMENT

Most organizations have adopted SaaS and PaaS solutions to simplify their IT footprint, have more predictable costs, and satisfy end-user demand for productivity capabilities. How your organization uses these web applications is a critical indicator of your security posture. Email specifically continues to be a considerable threat, with 90% of breaches incorporating some component of email within the attack. By determining user behaviors across these critical areas, we can help you understand one of the more prevelant cyber risks, and determine where you need to fortify your protections in this area.

APPLICATION AND DATA SECURITY

Most mid-sized businesses have a large footprint of custom databases, warehouses, and applications that are critical to their work. Some of these are internal applications, and some are directly user-facing. Either way, cybercriminals utilize and target look to attack these type of data-rich systems. Our assessment looks at the applications running on your network to ensure they follow secure software design and development best practices. Assessing the security of your databases, including role-based access control and secure configuration assessments, will uncover how difficult it is for hackers to get to your critical data.

CYBER INSURANCE 2023

2022 was an eventful year for cybersecurity teams as cyberattacks increased by 38%. This activity spurred cyber insurance companies to increase security requirements for businesses looking to obtain policies.

LEARN MORE

3 RISK FINDINGS REPORT & SUMMARY

THE FINDINGS

Once your assessment is complete, a summary of your technology and applications architecture and security vulnerabilities are outlined in a custom Cybersecurity Risk Assessment findings report. This report is not a checklist of the processes, policies, and defense measures you have in place; it is a robust summary of the business risks that are present within your IT operations, the competence of your current security measures, and gaps you may have in your defenses.

To communicate the efficacy of your security controls and their associated risks, we segregate controls into different categories and utilize a risk matrix chart (example *pictured below.*) This matrix helps to inform you of your maturity level for each cybersecurity control.

- **RISK** is calculated by considering a threat or vulnerability and evaluating the likelihood and impact of a compromise.
- **MATURITY** estimates how thoroughly and effectively your controls are deployed to mitigate risk.

Once this is determined, we calculate the remaining risk after the deployed controls' maturity have been applied. This is known as **RESIDUAL RISK** and is calculated:

RISK – MATURITY = RESIDUAL RISK

Residual risk is visually identified by a colorized maturity selection. In our risk matrix, we identify calculated residual risk with a low (green), medium (yellow), or high (red) risk level shown in the colorized selection of the MATURITY grade.

In the following example, the organization adheres to a "3" MATURITY level, indicating how well the control is implemented. The assessment team has determined that the initial RISK - MATURITY leaves the organization with low residual risk (green) in this control area.

GOVERNANCE, POLICIES, AND PROCEDURES

ACCEPTABLE USE AGREEMENT

1	2	3	4	5
No evidence.	- Developed but not current - Represents an older environment or practices - Lacks many topics typically found in an AUA - End-users were not aware of the document	- Developed and updated but contains irrelevant or dated material - Does not provide sufficient guidance in some areas of information security or platforms - Not reviewed annually by all staff	- Developed and periodically updated - May not be knowledged annually - May not cover some key areas	- Actively maintained - Users interviewed were aware of the agreement - Users knowledge annually

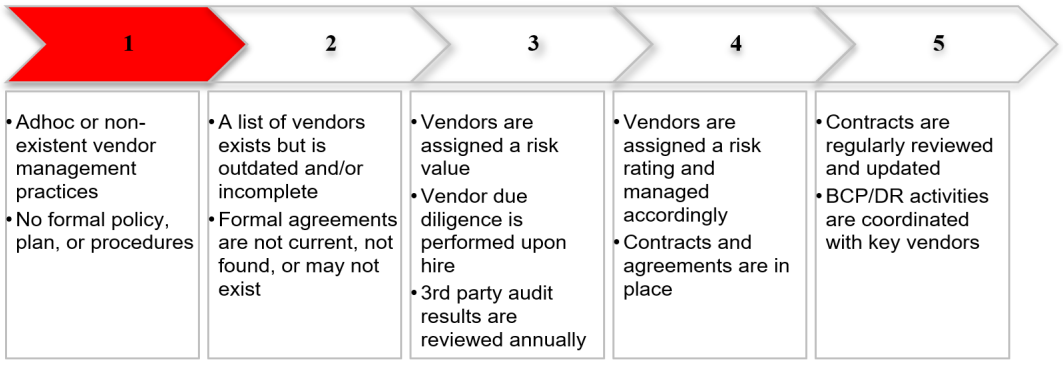
Risk Matrix Example

SYSTEMS engineering

CYBERSECURITY RISK ASSESSMENT REPORT
SAMPLE CONTROL FINDINGS

IT Vendor Management Policies

The organization increasingly relies on vendors to access, transmit, process, or store sensitive data and business transactions. Without a vendor management policy and program, organizations do not have the necessary assurances that vendors are exercising proper controls over their critical data and processes when in their custody.



MATURITY LEVEL

- Maturity Level Score: 1
- Security Risk: High

SUMMARY OF FINDINGS

There is no evidence of a formal IT vendor review process.

RECOMMENDATIONS

Develop a policy that includes the following major requirements:

- The maintenance of a comprehensive list of all IT vendors, including what goods or services they provide, maintenance agreements, and account information needed for support.
- Development of a criticality and risk ranking including importance to business operations and access to confidential data.
- Identify contract signature authority.
- Development of a process to ensure each vendor is reviewed for contractual requirements such as security controls, confidentiality agreements, acceptable SOC Reports, disaster recovery plans, and acceptable service level agreements (SLA). These reviews should be conducted on a regular basis with the frequency of review driven by the vendor risk rating.

In concert with the findings report, a risk overview presentation is given to business leadership summarizing the findings. This discussion provides professional perspective and offers high-level guidance to address the risks. The presentation is a business oriented, non-technical deliverable business leaders can utlize to prioritize risk and act.

The Cybersecurity Risk Assessment findings report includes:

- **Analysis regarding industry best practices and the existing IT resources and support model within the organization.**
- **Opportunities for improvement of high-value strategic initiatives**
- **Summary of solution recommendations to address areas where IT is presenting risk to the organization.**
- **Recommendations for improving the management of IT and hardening your security posture.**
- **When applicable, evaluation against your company's compliance requirements to identify compliance risks.**

SUMMARY

A cybersecurity risk assessment will help your organization it's ability to protect it's information and assets from cyber threats. A thorough review your security defenses will help you understand;

- **Your maturity level in each critical category of cybersecurity,**
- **Where gaps or missing protections lie within your current defense posture,**
- **The protections you have in place and if/how they are working,**
- **Your cyber vulnerabilities that need to be addressed,**
- **Where to invest your cybersecurity spend, and**
- **A proactive plan to help you PRIORITIZE and ACT.**

Cybercrime is on the rise. Cyberthreats, like ransomware and malware, are running rampant and are more persistent than ever. A thorough cybersecurity risk assessment is the fundamental first step in addressing your organization's IT risks and staying ahead of the bad guys.

ENABLING THE EXCEPTIONAL

Outstanding IT is more than equipment, systems, and process. It's a positive culture of understanding business objectives, and engineering frictionless technology solutions to meet them. We learn together every day, solving complex problems, and offering solutions that move us all forward. Our integrated technology solutions work seamlessly, securely, and intentionally, arming your organization with the tools and support you need to enable exceptional outcomes within your business.

888.624.6737 | systemsengineering.com | info@systemsengineering.com | Employee-Owned Company

4 SYSTEMS ENGINEERING

MOVING BUSINESS FORWARD SECURELY

Systems Engineering is a 100% employee-owned IT strategy and managed services provider. Our team of 180+ network engineers, managed security professionals, project managers, data management experts, and account managers are available 24×7, 365 days per year to meet the needs of our clients. From network design and installation to a full complement of managed IT, cybersecurity, and cloud services, we have an IT solution that enables your organization to grow and prosper.

IT SERVICES

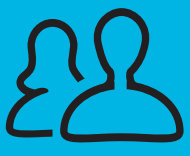
We deliver IT services that enable your business to be productive and grow. We help you responsibly invest in IT and security technologies that result in a stable, secure technology experience.

CYBERSECURITY

Our cybersecurity services and solutions combat the persistent threats businesses face every day. Our Security Operations Center (SOC) is on task day and night to monitor, detect, and respond to threats against your business.

CLOUD

We offer flexible, scalable managed cloud services, backed by our in-depth knowledge and experience to enable your company to maximize the benefits of your private, public, or hybrid cloud environment.



STRATEGY AND CONSULTING

We successfully navigate the evolving technology landscape, advising clients on how to align their business goals with technology. We solve complex business challenges and help clients leverage technology to achieve the business outcomes they desire.