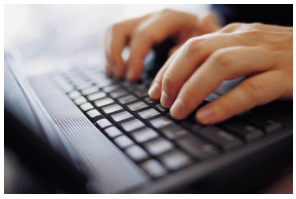
Cyber-Security Assessment

KEEP YOUR DATA SAFE WITH ENHANCED CYBER SECURITY

TACTICS NEED TO CHANGE

The recent rise in ransomware attacks and business-halting data breaches has made it clear that your organization must prioritize cyber security performance. But ad hoc security controls and defensive measures are not the answer. Instead, you need a strategic, risk-based approach with a cyber security road map as your guide.



Solutions for New Threats

In 2020, a staggering 31% of global companies were attacked by cyber criminals at least once per day. Over 1,000 had sensitive data stolen and publicly leaked by ransomware gangs. And even when a return to office life is possible, it seems clear that digital operations will remain far more prevalent than in previous years. online.

THE IMPORTANCE OF A CYBER-SECURITY ASSESSMENT

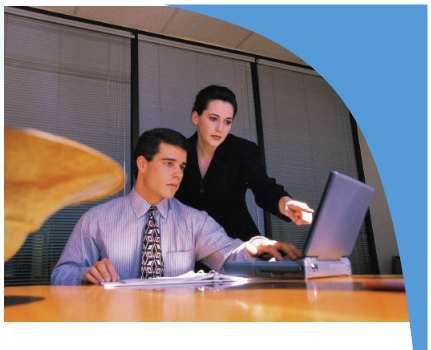
What is a Cyber Security Risk Assessment?
First, let's be clear what we mean by cybersecurity assessment. Like an annual wellness check-up for your health, this assessment aims to diagnose potential risks before something serious happens. This proactive assessment aims to detect or identify any system, network, software, device, physical, and other threats or vulnerabilities. The assessment findings help your business plan what it will do to respond to and manage the risk.
The depth and breadth of a cybersecurity assessment can depend on your business size, industry, risk threshold, timeline, and budget. Still, there are several signs suggesting your business needs to schedule a cybersecurity assessment soon.

Why carry out a cybersecurity risk assessment?
Risk assessment – the process of identifying, analyzing, and evaluating risk – is the only way to ensure that the cybersecurity controls you choose are appropriate to the risks your organization faces. Without a risk assessment to inform your cybersecurity choices, you could waste time, effort and resources – there is, after all, little point implementing measures to defend against events that are unlikely to occur or won't have much material impact on your organization. Likewise, it is possible that you will underestimate or overlook risks that could cause significant damage to your organization.

What does a cybersecurity risk assessment include?
A cybersecurity risk assessment identifies the various information assets that could be affected by a cyber-attack (such as hardware, systems, laptops, customer data, and intellectual property), and then identifies the various risks that could affect those assets. A risk estimation and evaluation is usually performed, followed by the selection of controls to treat the identified risks. It is important to continually monitor and review the risk environment to detect any changes in the context of the organization, and to maintain an overview of the complete risk management process.

INTELESYS
IT for Public Sector

Top Signs Indicating You Need a Security Assessment



Ransomware attacks are estimated to cost **$6 trillion annually by 2021**. 50% of a surveyed 582 information security professionals do not believe their organization is prepared to repel a ransomware attack.

#1 You've got a bad feeling that something isn't right.
Or you've seen something suspicious that makes you question your cybersecurity. This might be: Finding strange files on your network. Your computers are behaving in an odd way. Competitors knowing information about your company

#2 Regulatory compliance requirements
Your business may need to meet specific regulatory requirements. For instance, there are many rules about testing for cyber exposure in specific industries including financial, healthcare, energy, and educational settings. Compliance starts with a comprehensive cyber risk assessment, we are also able to make recommendations based on the results of your assessment to help your organization manage and maintain regulatory compliance.

#3 Your staff isn't tech-savvy
Insider threats remain one of the biggest cybersecurity issues. Your investment in security to lock down your "virtual house" doesn't help if your staff opens the door to anyone who knocks. Most employees don't intentionally open the organization to cyber threats. They just have poor computing habits. Some don't see a problem in securing their accounts (all of them) with a passcode such as "1234" or "password". Others are naive enough to actually believe an overseas prince wants to send them millions! Even the best trained employees can fall victim to business communications scams. Busy people may not notice when they get an invoice that looks exactly like a suppliers, but with a bad actor's banking details.

#4 Angry Former Employees
Depending on your size and the volume of work, you may not yet have a clear process in place for handling terminated employees' technology access. Are unhappy people quitting? Have you fired staff? Not everyone leaves on good terms, so revoke all former employees' access and change passwords. Providing former staff with continued access to your cloud-based platform is as foolish as exposing yourself to germs by waiting on the sick-patient side at the doctor's office.

#5 Old Technology
When possible organizations try to get more done with the tools we have rather than having to invest in and learn something new. Yet the "if it ain't broke, don't fix it" approach is not applicable to technology. Old software or operating systems are more likely to expose you to cyber risk. Once software reaches a certain age, the provider stops supporting that solution. Microsoft, for example, is phasing out security patches and updates for Windows 7. Don't plod along with decades-old technology, thinking you're safe because there hasn't yet been a failure or crash. The bigger danger is the small, unnoticed openings you don't know about, but cybercriminals do.

#6 No data control policies in place
The number of technology entry points on your network is always growing. There may be USB drives floating around your business environment holding essential data. Company laptops can be misplaced or stolen. Remote employees may sign on to unprotected Wi-Fi networks and portable devices aren't properly encrypted. Without policies in place to control data throughout your business environment, it's difficult to determine your vulnerabilities.

#7 Your employees use their own devices.

A Bring Your Own Device (BYOD) environment makes employees happy. The cyber criminals are pleased too. Sure, this approach can save money. Your business no longer has to ensure every employee has the latest available technology. But, there are drawbacks: Employee devices may not be the latest, which could make them more susceptible to cyber-attack. Staff could download malicious software or apps onto their personal devices that give cybercriminals access to your systems. Users may be entirely unaware their devices carry malware and could infect your systems when connected. The employee may not be the only user of the phone which has access to business information. Disgruntled employees can use their own devices to damage your network.

What's Included in The Assessment

A vulnerability assessment is **a systematic review of security weaknesses in a network environment**. It evaluates if the system is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, potential impact on systems, and recommends remediation or mitigation, if and whenever needed.. Each Assessment consist of:

- ⇒ Installation of a secure data collector to track vulnerabilities over time
- ⇒ One week's collection of data
- ⇒ Testing to identify vulnerabilities on the network
- ⇒ Assembly of vulnerabilities collected with severity rating
- ⇒ Detailed reporting of issues discovered
- ⇒ Suggested mitigation solutions for vulnerabilities where available
- ⇒ Credentialed and credentialed scans available
- ⇒ Mitigation services available upon request
- ⇒ NIST, CMMC, HIIPA assessments available

◊

Estimated global losses from cybercrime are projected to hit just under a record $1 trillion for 2020 as the coronavirus pandemic provided new opportunities for hackers to target consumers and businesses.

(Washington Post)

ASSESSMENT COSTS

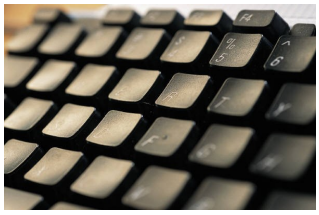
1-199 Users:	$1,995*
199-499 Users:	$2,995*
499—1,999 Users	$4,995*
2,000+ Users	Ask for Quote

*Pricing does not include vulnerability Mitigation.

Ask for special government pricing options!

Map Your Path to Security

Before you rush to invest in the latest and greatest new security controls, refer to your cyber security roadmap. Think of it as a strategic guide that can help you gain a clear, data-driven understanding of risk. With these insights, you can better align your security program with business goals, prioritize security investments, measure success, and continually improve.



100% Satisfaction Guarantee

We are so confident our assessment will deliver exceptional value that we make this pledge to you—If for any reason you feel the information we present is not valuable or useful to your organization, you will not be billed for the service

NO QUESTIONS ASKED!

Other Available Services

Network Assessment

Our team of CJIS certified engineers will identify all components on your network and provide you with a complete system inventory. They will also audit traffic flow and determine any bottlenecks or routing issues.

IT Project Outsourcing

Have a list of backlogged IT projects? Whether you need a Exchange migration to the cloud or a server farm upgrade, the professionals at Intelesys can augment your team to get on top of you priority initiatives!

Managed Services

IT costs skyrocketing in your organization? Flat rate, fully managed IT services might be your answer! Free your technical team's time to manage vendor relations and end user improvement, leave the network infrastructure to us.

Security Training and Auditing

It's a well-known fact that most security breaches stem from human error. In today's active cyber-security world it is imperative for staff to be consistently trained and audited for proper cyber hygiene. Let our Intelesys trainers handle this critical function for you!

INTELESYS
IT for Public Sector