

How to Implement an Effective Cybersecurity Solution

The Critical Attributes of Risk Management and Cybersecurity

BY **NETCOM** LEARNING

Contents

INTRODUCTION	3
TOP 5 CYBERSECURITY THREATS AND VULNERABILITIES	4
YOU DON'T WANT TO BE THE NEXT VICTIM OF CYBERCRIME	6
THE 7 STEPS TO REDUCE SECURITY RISK	7
MANAGING RISK AND SECURITY AT THE SPEED OF DIGITAL BUSINESS	9
CYBERCRIME ON THE RISE – WHAT TO DO?	11
HOW TO MANAGE RISK, BUILD TRUST, AND EMBRACE CHANGE	12
RESILIENCY TO ACHIEVE HIGH RELIABILITY	13
SUMMARY AND FINDINGS	14

Introduction

From cyberattacks and hacking to phishing and device failure, your information is always under threat. That is, unless you have a robust and effective Risk Management and Cybersecurity system in place that is constantly reviewed and upgraded.

The recent high-profile cyberattacks involving the WannaCry ransomware reportedly affected more than 230,000 computers across 150 countries. Despite claiming to have adopted high-profile security algorithms, many IT giants, including Facebook and Twitter, have also had their information compromised recently.

As quickly as economies are adopting digital systems to manage their transactions, the rate of cybercrimes is also increasing. Even the latest, proven cybersecurity systems have failed before such cyberattacks. It is not only about information intrusion, but also about large sums of money being lost due to cybercrimes. Businesses are losing customers and client trust because of the increasing number of cybercrimes to which people are subjected every day.

We have come to understand that there is no one-size-fits-all to counter cybercrimes. Cybersecurity solutions need to be customized to every business for the best performance.

Top 5 Cybersecurity Threats And Vulnerabilities

Just as the world was going gaga over bitcoins and their supposedly secure payment gateway, the WannaCry Ransomware attack gave a tight slap to those who believed that bitcoins were quite safe to deal with. In fact, it turned out to be just the opposite! This attack has made organizations think more seriously about the vulnerabilities of their information servers. The idea is to protect the information stored on the company server from virus or ransomware attacks.

Surveys showcase the sharp increase in the levels of cyberattacks occurring every year in spite of the increasing amount organizations spend on security tools and software. Cybersecurity is not only about the tools that you invest in. It is more the information security strategies that you adopt and the vendors that you partner with that matter. Organizations should expend some effort on identifying their vulnerabilities. There are risks that are known and can be countered, and there are risks that are unknown and need to be identified more seriously. The most vulnerable security aspects remain in the unknown area, as the organization has no clue what to expect. Here are some of the known threats to a vulnerable cybersecurity system:

Leaked Information – Information can be leaked from an organization in many ways. The source of intentional leaks is difficult to identify, but the leak can be identified and blocked. Classified information may be leaked while it is being transferred between servers or while browsed. This often happens, in part, because the SSL certificate verifications are not done or the SSL errors are ignored.



Poor Authentication and Session Management - This can only happen by overlooking the basics of cybersecurity. When the website fails to hide the password and session objects, they are quite easily open to hackers. This is like inviting the attacker to hack and steal all the information they have.

Crimeware and Malware - Tools and Trojans that provide remote access to computers can be a huge threat to security. Keyloggers can capture the keystrokes to steal the password and use the employee logins to access critical information without the organization even knowing it. Ransomware like WannaCry has already proven quite expensive for many organizations in recent days. Malware attacks happen when malicious links are clicked or software downloaded and installed.

Crypting - The viruses and malware are encrypted such that the antivirus software fails to identify it as a potential threat. This way, the hackers can install malware or virus easily on their target machines without being detected.

Obsolete Software - Outdated software, unchecked authorities, applications running in debug mode, configuration and default account settings – all can be lethal to cybersecurity.

You Don't Want to be the next Victim of Cybercrime

Forbes suggests another massive ransomware outbreak is going global fast. Over the past few months Honda, Kmart Stores, US drug maker Merck & Co, and largest power companies have been bearing the brunt of what appears to be a massive ransomware outbreak that's fast spreading across the world and hitting a significant number of **critical infrastructure providers**.

Few samples of data breach in the recent past and losses it lead to:

U.S. Department of Justice

February 9, 2016: Hackers angry about U.S. relations with Israel tried to call attention by breaching the U.S. Department of Justice's database. [CNN reported](#) the hackers released data on 10,000 Department of Homeland Security employees one day, and then released data on 20,000 FBI employees the next day. Information stolen included names, titles, phone numbers, and e-mail addresses; the Department of Justice does not believe that any sensitive information, like Social Security numbers, was obtained.

Internal Revenue Service

February 29, 2016: The Internal Revenue Service (IRS) announced that the data breach they uncovered in May 2015 was [much larger than initially believed](#). In May, the IRS said over 100,000 American taxpayers had their personal information compromised when the agency's "Get Transcript" system was hacked. However, in February 2016, those numbers have been increased to over 700,000. The IRS thinks a sophisticated Russia-based criminal operation is responsible for the data breach and that identities were stolen to file fraudulent tax returns in the future.

Yahoo

December 14, 2016: Less than three months after announcing a [2014 data breach](#) that affected 500 million users, Yahoo did it again — and even bigger than before. In December, the company discovered [another breach](#) from 2013 that may have compromised the personal information of one billion Yahoo accounts, making it the largest data breach in history. At the time of the breach announcement, Yahoo did not have much additional information to share with the public, as it was still unclear who was responsible, how they got into the system.

The 7 Steps to Reduce Security Risk

While most medium and large businesses are aware of their vulnerabilities and take at least the basic cybersecurity measures to protect their information, small businesses are typically ignorant of the need and hence fall prey to frequent and damaging cyberattacks.

Ensuring cybersecurity, or at least reducing the risks, involves taking the following steps:

- 1 Analyze the Security Risk:** Every organization has a different set of security risks. With a competent team of security analysts, the threats first need to be analyzed in detail.
- 2 Draw up a Detailed Plan to Cover the Risks:** Once the risks are analyzed in detail, the security partners or the team can draw up a detailed plan to cover those risks already identified.
- 3 Estimate the Unidentified Risks:** What remains unidentified poses a bigger threat to security, as the organization has no clue what can go wrong to be prepared to counter it. Hence, it is important to identify the level of unknown risks.
- 4 Combating the Unknown:** Though the unknown remains not known, once the level of what remains to be identified is known, a detailed contingency strategy can be drawn that would lessen the effect of an unknown risk.

- 5 **Security Strategy:** A detailed security strategy needs to be drawn to serve as the basis for different departments handling critical information.
- 6 **Security Compliance:** Every piece of information dealt with in the organization should conform to the security policies laid down by the cybersecurity experts. This has to be strictly followed to make sure there are no loopholes concerning the known risks.
- 7 **Security Audits:** Internal and external audits can be carried out periodically depending upon the criticality of the information at stake. This will keep check on the updates and upgrades required on cybersecurity from time to time.

The key is to identify all potential threats and understand the level of unknown threats. The strategies have to be formed based on the business priorities, which have to be clearly laid down in black and white. These policies should address all possible aspects of information security, including internal usage, external usage, incident management, configuration management, user privileges, and network security. The instructions should be strictly followed to ensure minimal risks in the known sector. As for the unknown threats, create awareness among the users so that they will be vigilant about the information they handle.

Managing Risk and Security at the Speed of Digital Business

Understanding vulnerabilities, estimating security measures, and adopting rigid cybersecurity policies become even more important for digital businesses. Digital businesses have significantly changed the global economy. Fewer people are engaged in traditional businesses or benefit from them, as more businesses embrace digital technology to empower their business capabilities. But with that shift comes cybersecurity vulnerability, which keeps evolving, just as the technology keeps evolving. Apart from technology, other areas in a digital business also need to be addressed in order to combat cybersecurity threats. Areas that should be monitored include:

People Patterns

Just as the technology is forever evolving, people's behavioral patterns are also forever changing. It is important to closely watch the people patterns, be it your employees' or your customers', when you are analyzing cybersecurity risks.

Processes & Technology

Just as the cyber threats are ever growing, a company's processes and technology need to be flexible enough to adapt to the changes necessary for countering the evolving patterns of cyberattacks. It is important to walk at least one step ahead of potential attackers by changing your processes and technology periodically.

Always have a Plan B

There's always the danger of an unknown risk factor. Keeping this in mind, it is important to always have a backup plan or a Plan B, just in case Plan A fails. This is perennially important for the IT sector, as they are the most vulnerable.



Protect Outsourced or Shared Assets

Since most information and business processes are outsourced or shared, services such as SaaS and PaaS are increasingly used; the organization no longer owns them exclusively. This poses a much bigger threat. A detailed risk analysis must be done on the outsourced and shared services used by the organization.

Plan for the Unknown

Digital businesses have more unknown lethal threats than known ones. When the attacker targets a totally unprotected area, the consequence can be tragic as it is an unexpected blow.

Since digital businesses arise much faster than traditional businesses, the risk attached is definitely on the higher side. The key is to closely watch the business and the information it generates so as to identify any potential risks. In particular, monitor behavioral patterns and critical information from IoT because IoT adds an additional element of vulnerability. Digital businesses operate in a continually evolving environment, which adds to their risk. Understanding the level of unidentified risks will help the risk management team be better prepared for any hazards.

Cybercrime on the Rise – What to do?

Coinciding with a yearly rise in the number of businesses going digital has been a precipitous rise in the number of cybercrimes. In fact, cybercrime has increased by a staggering 95% in the last 6 years. It involves more than \$110 billion in loss to customers and more than \$12 million to the US companies affected. For digital businesses, it is one of the most worrying problems to tackle. In addition, the personal information of more than 22 million people has been compromised, resulting in a public frenzy. The situation looks even more threatening in light of recent surveys revealing that scarcely 40% of IT companies seem to be prepared for cybersecurity attacks. As far as non-IT businesses are concerned, it is only a matter of time until they realize the massive effect of a security breach that could have been easily identified and blocked.

One of the major reasons for security breaches is a lack of awareness among employees who deal with critical information. Having a strong IT security standard and policy in place is not enough to tackle cybersecurity issues. Generating awareness and training the staff in advanced IT security measures are important, too. At present, however, it is difficult to find many professionals adequately trained in advanced cybersecurity installation and standard settings. Corporate training in cyber safety should be provided to all employees who deal with critical information.

Manage Risk, Build Trust, and Embrace Change

Training helps organizations to understand and adapt the latest technologies in the most effective way to combat cybercrimes. Training on cybersecurity risk management is a continuous process. In an ever-evolving digital world, businesses must be vigilant in keeping track of relevant trends and changes. Due to frequent bouts of virus and malware attacks, stakeholders and customers are becoming increasingly wary of digital transactions and businesses. To regain their confidence and trust, it is important for businesses to adopt the latest cybersecurity measures, including training personnel about the need to be vigilant toward cybercrime. NetCom Learning provides your business end-to-end cybersecurity training, which will help fill any gaps in risk management and prepare your staff for more secure information management.

IT security training can help all businesses deal better with security risk management. Continuous learning raises the level of understanding about changing IT and business environments, and with NetCom Learning your business can leverage the expertise of qualified, experienced trainers who have ample hands-on experience in managing cybersecurity. It is important to learn from experts with the experience to address large-scale information and security issues. Expert training ensures that your staff will leverage years of industry experience to defend and prevent cyberattacks. NetCom Learning helps you create a learning culture, learning plan, and learning operation to create a long-term impact on your employees.

Resiliency to Achieve High Reliability



Training prepares your employees to build resilient systems, which are more important than robust systems in a risky cyber world. The flexibility to change and adapt to the changing environments of IT security is what makes systems resilient. This flexibility can only be achieved when your staff is equipped to adapt to change. Resilience is the most important factor for survival in a volatile and risky cyber world. People, resources, and technology should all be flexible enough to adapt to the changing environments of cybersecurity and be able to defend against known and unknown attacks.

Summary and Findings

Cybersecurity is fast becoming one of the major threats to digital businesses. The increasing pace of cybercrime, along with its multifold impact, threatens the existence of technology. The recent, well-publicized cyberattacks confirm the need for better cybersecurity strategies that involve

- Customized risk assessment and security strategies for every business
- Continuous analysis and update of security standards and policies
- The need to conform to established policies and standards
- Understanding the intensity of unknown risks
- Building a resilient structure to quickly adapt to changing situations
- Being responsive to even the slightest changes in behavioral patterns
- Training your staff in cybersecurity risk assessment and management

The shift from technology to people is essential for combatting cybersecurity issues. Training prepares employees to understand the importance of security, encourages them to comply with security policies, makes them aware of the need to be vigilant, and instructs them in how to control the damage in case of a security breach. Expert training from a pioneer like NetCom Learning is the perfect solution to resilient and reliable systems that can quickly adapt to changing cybersecurity requirements.

NetCom Learning helps build innovative learning organizations in the workplace by structuring a smarter workforce, supporting changes, and driving growth. Since 1998 we have been empowering organizations to reach optimal performance results and address challenges by managing all aspects of organizational learning.

Learn more at www.netcomlearning.com

