White Paper
2016

Cyber Security and Compliance

Protecting your network and playing by all the rules.

A guide to complying with NERC CIP, HIPAA and DSS regulations.

A Publication from sath

Table of Contents

Introduction

Cyber security and compliance management within an organization is becoming more and more of a prevalent matter. With more organizations being breached either due to out dated cyber security practices in place or organizations not keeping up with the necessary compliance measures set by NERC CIP, HIPAA, DSS, FFIEC, SOX or PCI. Organizations are now starting to place more emphasis on making sure these issues become less frequent and if by some chance a breach happens the proper measures are in place to limit the damage.

Cyber security with an organization is now starting to become more of a C-level initiative instead of just being lumped under all other IT issues. The magnitude of a breach and the rising cost per file compromised has caught the attention of C-level executives and it is no longer an issue they can briefly discuss or assume it is a matter handled by the IT department. Actions and measures taken need to be updated and upgraded to face and handle the constant attacks many organizations face on a daily basis.

Compliance rules and regulations like NERC CIP, HIPAA, DSS, FFIEC, SOX and PCI set within a particular industry are changing at a more rapid rate than years past. The reason for this change is the constant evolution of technology and the ever more dependency on this technology in our daily lives. Making sure that the bare minimum is at least being done to protect these technologies and the customers who depend on it is a matter all organizations must pay attention to. Organizations need to make sure they are compliant with from the start and not addressing it once they become non-compliant.

What is cyber security?

Cyber security focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction. Governments, military, corporations, financial institutions, hospitals and other businesses collect,

> "With the growing volume and sophistication of cyberattacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security."

process and store a great deal of confidential information on computers and transmit that data across networks to other computers and must have measures in place to protect it. With the growing volume and sophistication of cyberattacks, ongoing attention is required to protect sensitive business and personal information, as well as safeguard national security. An organization can no longer work under the idea that my organization is too small for a hacker to want to attack my network. Every organization, at one time or another, will fall victim to a breach and must have the proper safeguards in place to protect their system and network as well as the ability to minimize and fix the damage once they are breached.

What is compliance?

Compliance is the processes and internal controls put in place by such entities like NERC CIP, HIPAA, DSS, FFIEC, SOX and PCI, that an organization must meet. The requirements are imposed by government bodies, regulators, industry mandates or internal policies. An initiative to comply typically begins as a project. Organizations will race to meet deadlines to comply with these rules and regulations. These projects will consume significant amounts of resources as meeting deadlines become the most important objective. Organizations need to realize that compliance is not a one-time event. It needs to be made into a repeatable process, this way you can continue to sustain compliancy with the rules and regulations at a lower cost than the first deadline. The simplest way to comply is to only follow the rules that have legal consequences for noncompliance and then only meet the minimum requirements to avoid the fines and penalties. However, many firms are starting to go beyond this approach to mitigate risk and create a defensible strategy in the event of falling to being noncompliant. When organizations are dealing with the regulations set by their industry a streamlined process of managing compliance with each and every one of the initiatives is critical. If not managed and monitored the costs can spiral out of control and the risk of being non-compliant increases. The compliance process enables organizations to be compliant repeatedly and this will enable organizations to sustain it

"Organizations need to realize that compliance is not a one-time event. They need to make it into a repeatable process."

on an ongoing basis, at a lower cost and decreases the chances of them becoming non-compliant.

The evolving world of cyber security and compliance

Cyber Security

Cyber security use to as simple as just setting up a wall on the perimeter of your system and that would be enough to keep the bad guys out. Today though if you just set up a perimeter you are not even considered to be doing the bare minimum. Today, you also need to make sure the inside of your network is protected from those who are already on the inside. Cyber security in the past was seen as only an IT department issue whereas today it is now a C-level decision. The reason for this shift is not just the fact that more and more large organizations are being breached and these organizations do not want the negative press but because the sophistication of the bad guys is out pacing the solutions in place. This is forcing organizations to stay nimble and to be able to protect against a far more vast range of challenges, unlike those in the past. Organizations must continue to review and evaluate what they have in place and decide if they should look to an upgraded solution. Another major change is where the system you are protecting is being utilized. In the past all things tied to the organization's system and network was located in one location, your offices but today many organizations have computers, tablets and cell phones on their system and network but these electronics are not tied to your office. This creates new challenges that did not exist years ago.

"Cyber security use to be seen as only an IT department issue whereas today it is now a C-level decision."

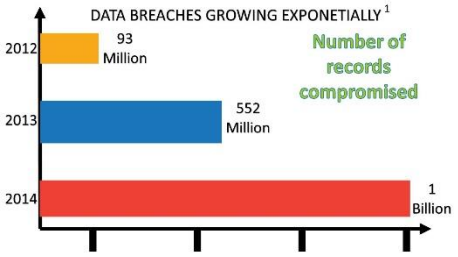
Compliance

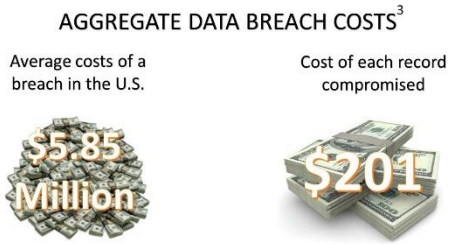
The explosive pace at which industrialization and technological advancements have seen over the past years has exposed many systemic weaknesses that can arise from an increasingly complex global industrial infrastructure. The combination of human competencies with other factors such as computer systems, heavy machinery, chemical or nuclear engineering, has demonstrated, through a series of unfortunate events, that unforeseen risks can be a contingency of modern business operations.

Major industrial and financial catastrophes such as the sinking of the Titanic, Chernobyl, Three Mile Island, Enron, the BP oil spill and London Whale are just a few examples of what has contributed to the growing need for a formal strategy to combat and prepare for known and unknown risks. Many of these incidents have led directly to legislation that's designed to insulate the public, environment, and economy against future disasters similar in nature. Many federal workplace regulations, building codes, privacy laws, environmental safety standards, banking reforms, and financial reporting mandates have been enacted in the aftermath of disastrous events.

The cost of ignoring cyber security

Gone are the days where the only security issue organizations had to worry about was someone trying to break into their facility and making off with merchandise. Today, the security issues majority of organizations face is someone trying to break into their computer system or network and make off with confidential files and information. This new security issue has been on the rise over the past ten years and has been growing exponentially over the past five years.





1. Steve Ragan, Nearly a Billion Records Were Compromised in 2014, CSO (Nov. 17, 2014) http://www.csoonline.com/article/2847269/business-continuity/nearly-abillion-records-were-compromised-in-2014.html.
2. Internet Security Threat Report 2014 (2013 Trends, Volume 19) Symantec Corporation (2014) https://www.symantec.com/content/en/us/enterprise/other_ resources/b-istr_main_report_v19_21291018.en-us.pdf.
3. Research Report, 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute (2014).

An example is seen in the growth of data breaches from year 2012 to 2014. In 2012 ninety-three million files were compromised, then in 2013 five hundred-fifty two million files were compromised and then in 2014 one billion files were compromised, that is an eighty-one percent increase from 2013 to 2014 and that number continues to grow as thieves and the technology gets better. It is estimated that annually the cost of the impact of theft of intellectual property is somewhere between two hundred and two hundred fifty billion dollars and could cost upwards of two hundred thousand jobs.

Globally the estimated annual cost is upwards to five hundred thirty-eight billion. The cost per hour of distributed denial of services attacks is around one hundred thousand dollars. An organization cost of a breach on average in the United States is around five million eight hundred five thousand dollars. The average cost per file that is compromised in the United States is around two hundred dollars. These costs do not factor in the costs associated to the measures that organizations must take to restore the identity of those who have their files compromised. This can be done through credit monitoring services, creating a new pin number for tax filing purposes or even financial compensation due to identity theft suffered by the victim.

A perfect example of a breach that could have been avoided had basic cyber security updates been done is the breach with Office of Personal Management (OPM) within the US government. In the summer of 2015 it was discovered that the OPM had a data breach. Initial reports were that four million records of current and former civilian agency and military employees were leaked but when the dust had settled and the investigation concluded that four million ballooned to twenty one and a half million records compromised, with five million six hundred thousand finger print records compromised. The reason those who hacked the system were able to get all those records was because the data stored on the OPM's system was not encrypted and it was not encrypted because the system was out of date. So once the hacker was able to gain access onto the system their ability to extract records was easy were as if the system was up to date the records would have been encrypted thus making it a lot harder to decipher the information extracted. The fallout from this negligence was huge. First the Director of the OPM, Katherine Archuleta, was forced to resign from her position. Secondly, the government paid twenty million to a firm that would notify the four million people first reported along with eighteen months of credit monitoring. Then five months after the breach was publicly disclosed the government paid an additional one hundred thirty-three million to a firm to notify the remaining victims along with three years of credit monitoring and identity-theft prevention services. That is over one hundred fifty million dollars just to help monitor the victim's identity.

"It is estimated that annually the cost of the impact of theft of intellectual property is somewhere between $200 and $250 billion dollars"

The government also needed to address the systems and all the problems that it had. U.S. Chief Information Officer, Tony Scot, called for immediate updates and patches of all systems which was called the 30-day cybersecurity sprint. What this entailed was:

- "Immediately" deploying so-called indicators, or tell-tale signs of cybercrime operations, into agency anti-malware tools. Specifically, the indicators contain "priority threat-actor techniques, tactics and procedures" that should be used to scan systems and check logs.
- Patching critical-level software holes "without delay." Each week, agencies receive a list of these security vulnerabilities in the form of DHS Vulnerability Scan Reports.
- Tightening technological controls and policies for "privileged users," or staff with high-level access to systems. Agencies should cut the number of privileged users; limit the types of computer functions they can perform; restrict the duration of each user's online sessions, presumably to prevent the extraction of large amounts of data; "and ensure that privileged user activities are logged and that such logs are reviewed regularly."
- Dramatically accelerating widespread use of "multifactor authentication" or two-step ID checks. Passwords alone are insufficient access controls, officials said. Requiring personnel to log in with a smartcard or alternative form of ID can significantly reduce the chances adversaries will pierce federal networks, they added, stopping short of mandating multi-step ID checks.
- A "Cybersecurity Sprint Team" was created to lead a month-long review of federal government's security hygiene practices.

The cost of ignoring being compliant

A high-skilled, high-quality compliance function is expensive to build but it will be one of the best investments for a firm and its senior managers. With some fines and penalties being as much as a million dollars a day, firms cannot afford to be non-compliant. Many firms have employed more compliance staff but there is a growing need for more truly skilled compliance officers. A consistency of expectation that the cost of skilled compliance staff will continue to rise, but the growing issue is in the availability of high-quality skills and experience. Many firms are expecting skilled staff to cost more due to the high demand and limited pool of applicants. The major reason for the expected increase in the cost of senior compliance professionals is the demand for highly skilled and knowledge staff.

"With some fines and penalties being as much as a million dollars a day, firms cannot afford to be non-compliant."

There's no doubt that compliance is a burden and that some of the activities organizations are required to demonstrate to be compliant with the rules and regulations don't always directly contribute to the security of the organization. The reality is the cost of regulatory compliance does not have to be expensive, but it's often made that way. This is because people are rushing to put things in place to meet deadlines and please their auditors. They are not actually thinking of being compliant as a whole or how developing a long term plan and solution is more beneficial for their organization.

Why organizations need to focus on their cyber security and compliance

Everyone understands the costs associated to not being cyber secure or being compliant with all the rules and regulations. However, one factor is sometimes over looked by organizations and can be just as important as the cost and that is how the organization is viewed by the public when it is reported there has been breach. Brand reputation is something that takes many years of great service and products to build but only one bad news story to severely damage. Examples of organizations that had to deal with this kind of negative press are Target, Home Depot, Sony, and the US government to name a few. Each of these organizations suffered a breach by either not making sure their system or network was as secure possible or because they neglected rules and regulations that would have met the basic requirements to be compliant. As a result they had to suffer weeks of the press digging into the details of the breach and discovering all the things the organization did wrong and neglected. Also discovered were all the things the organization didn't have in place prior to the breach to make sure the something like that that didn't happen. Costs associated to updating and patching your organization's cyber security, costs associated to your organization being compliant, cost associated your brand when there is a breach and the cost associated to repairing those effected by the breach are all reasons an organization needs to be up to date with their cyber security and compliance.

> "Brand reputation is something that takes many years of great service or products but only one bad news story to severely damage."

Conclusion

Everyday their seems to be more people looking to cause havoc by gaining access to an organization's system or network to either stealing important confidential information or holding the system or network for ransom. Because of this it has never been more important for an organization to be up to date with their cyber security measures and being compliant. The decisions made about these areas are no longer seen as just an IT

department issue but something that the C-level executives decide on. Security measures done in the past are no longer adequate to protect your organization, more measures must be in place to insure that both inside and out are secure from any wrong doers and practices in place to minimize the damage when a breach happens. Also, it is no longer acceptable to avoid being compliant because it does not add value to what your organization does. Being compliant with the rules and regulations set by your industry is just the bare minimum an organization can do. A long term solution to minimizing the costs associated to make sure your organization is compliant is a practice many organizations are starting to implement. The best way to avoid a breach is to continually evaluate your organization's cyber security and install patches and upgrades while also streamlining processes to make sure your organization is compliant and continually meets compliancy requirements.

About Sath Inc.

Sath Inc. is your place for IT Security and Regulatory Compliance. Established in 2004 we help our customers implement industry leading technical and business solutions for governing, analyzing, auditing and operating on everything related to IT security and compliance. At Sath, we create meaningful connections with our clients through strategic and sustained engagements and innovations in IT security compliance and governance space. Above all we believe in attention to detail, interaction, experimentation and continuous improvement. We deliver intelligent services, security assurances, thoughtful processes and exceptional outcomes for our incredible clients all over the world.

If you would like to know more about how Sath can help your organization with your cyber security and compliance issues,

Visit us at:

Sath.com

Or contact us at:
marketing@sath.com