Cybersecurity

Insurance Policy

3rd Party Assessment of Compliancy

Version 1.2 ● 23 November 2021

K2 Tech Group, Inc – 121 Executive Center Drive, Suite 138, Columbia, SC 29210 – 803.828.7871 – support@k2techgroup - https://k2techgroup.com

© 2021 K2 Tech Group, Inc. All rights reserved.

K2 Tech Group, Inc. 121 Executive Center Drive, Suite 138, Columbia, SC 29210

803.828.7871 https://k2techgroup.com

Trademarks

K2 Tech Group, Inc. are registered trademarks of K2 Tech Group, Inc. All other trademarks or registered trademarks are the property of their respective owners.

Disclaimer

The information provided in this document is provided "as is" without warranty of any kind. K2 Tech Group, Inc. disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall K2 Tech Group, Inc. be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if K2 Tech Group, Inc., or its suppliers have been advised of the possibility of such damages.

Document Lifetime

K2 Tech Group, Inc. may occasionally update online documentation between releases of the related software. Consequently, if this document was not downloaded recently, it may not contain the most up-to-date information. Please refer to https://k2techgroup.com for the most current information.

Where to get help

K2 Tech Group, Inc. support, product, and licensing information can be obtained as follows.

Product information — Documentation, release notes, software updates, and information about K2 Tech Group, Inc. products, licensing, and service, are at K2 Tech Group, Inc. website at:

https://k2techgroup.com

Technical support — Go to https://K2Techgroup.com and select Support. On the Support page, you will see several options, including one for making a service request. Note that to open a service request, you must have a valid support agreement.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this document to:

jgarrison@k2techgroup.com

If you have issues, comments, or questions about specific information or procedures, please include the title and, if available, the part number, the revision, the page numbers, and any other details that will help us locate the subject that you are addressing.

Table of Contents

© Company 2021. All rights reserved

1 Introduction

With the increased malware and ransomware attacks targeted against corporations, small businesses and government entities, Cyber insurance claims have increased 2.4% since last year. Targeting small and mid-sized businesses with 250 employees or less, the frequency of claims has increased 57% (Coalitioninc, 2021). Cybersecurity policy carriers are at the forefront of an expanding net of customers being attacked, and suffering data loss including personal identifying information.

1.1 Purpose

This paper will identify the need for a baseline compliance assessment, for which industry(ies) the client business falls in and conducting an assessment health finding in the client's infrastructure, physical security, cybersecurity, and other insurance carrier's risk areas. Only then can the known risk be assessed, and the risk shared.

As the industry has seen in nation-state attacks and breaches in 2020-2021, the perimeter is no longer the drawbridge into the entity being protected, but against those endpoints within. Apart from the physical and cyber aspects of risk management, there is the human factor that has the highest risk and threat to a business' survival during these attacks.

© K2 Tech Group, Inc. 2021. All rights reserved.

1.2 References

Align.com, 18 Nov 2021, https://www.align.com/blog/6-reasons-why-businesses-need-cyber-security-awareness-training

Cisco.com, 18 Nov 2021, Coalitioninc.com, 15 Nov 2021, "https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf"

Coalitioninc.com, 15 Nov 2021, "https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2021-07-Coalition-Cyber-Insurance-Claims-Report-2021-h1.pdf"

Dept. Homeland Security (DHS), 21 Oct 2021, "https://www.stopthinkconnect.org"

Gartner, 21 Oct 2021, "https://www.gartner.com/en/documents/3980891/the-urgency-to-treat-cybersecurity-as-a-business-decisio"

GIAC, 18 Nov 2021, https://www.giac.org/paper/g2700/1212/framework-building-comprehensive-enterprise-security-patch-management-program/111066 "

Identity Management Institute, 18 Nov 2021, https://identitymanagementinstitute.org/security-challenges-of-remote-workforce

Microsoft, 21 Oct 2021, "https://www.microsoft.com/en-us/microsoft-365/business-insights-ideas/resources/cybersecurity-small-business"

Microsoft, 16 Nov 2021, "https://docs.microsoft.com/en-us/compliance/regulatory/offering-home"

© Company 2021. All rights reserved

Mimecast, 18 Nov 2021, https://www.mimecast.com/content/email-scanning/

NIST, Information Technology Laboratory/Applied Cybersecurity Division, 18 Nov 2021, "https://www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication"

NIST, Small Business Cybersecurity Corner, 21 Oct 2021, "https://www.nist.gov/itl/smallbusinesscyber"

SANs Institute, 19 Nov 2021, A Practical Guide to Enterprise Anti-Virus and Malware Prevention. https://sansorg.egnyte.com/dl/Wee4v5snSb

Small Business Administration, 21 Oct 2021, "https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats"

Secure Controls Framework, 18 Nov 2021, "https://www.securecontrolsframework.com"

© K2 Tech Group, Inc. 2021. All rights reserved.

2 Cybersecurity

2.1 Regulatory Compliancy

Many small businesses go through their days without thinking about a security breach, physical or Cyber related. Not having an alarm system or Cybersecurity can cost a business money, time and quite possibly, result in lost information, and even the business' reputation (Microsoft). Most small businesses (less than 100 employees) can't afford a dedicated Information Technology department, and if they have 1 or 2, that company most likely will not be able to afford training, or equipment budgets for keeping up with the industry standards or compliance requirements.

Every business - enterprise, large, or small, will need to be in compliance of at least one industry regulatory rule, or more. There are at least 40 different industry-specific regulatory compliance offerings, many have overlapping requirements, some are more specific. There are compliance requirements spanning the globe, regional areas and governmental regulations for each country a business operates in (Microsoft).

With that large number of areas of industry-specific requirements, it is a far-gone conclusion that any number of businesses will be non-compliant, and at risk.

© Company 2021. All rights reserved

3 Cybersecurity

3.1 What can be done for Risk Mitigation before a claim?

A baseline risk assessment would be beneficial for all parties concerned, which includes physical and Cyber, the plant information technology (IT) infrastructure, disaster recovery, and storage, etc.

Prior to the issuance of a Cybersecurity policy, an auditing firm should conduct a baseline risk assessment, their findings can be made part of the policy for reference. The insurance carrier can then mandate to the policy holder or potential customer what is needed in order to obtain a Cyber Insurance policy. In the case of a claim, the state of the policy holder's IT infrastructure would be documented; before the Cyberattack (loss) and subsequent claim. With the knowledge that the auditing firm verified or discovered compliance/non-compliance, the insurance carrier would be protected in either regard, and so would the policy holder.

Training for identifying phishing, spear-phishing and other emails containing malware/ransomware would be of great value and a high-risk mitigation, prior to a security breach or encryption. People (employees) are the weakest link in the overall security posture of any business, being unaware of attack methods of social engineering and email scams (Microsoft). Having training in identifying scams, email headers to verifying the sender, and the current social engineering methods of spammers and hackers, would be of benefit to the policy holder and insurance carrier.

© K2 Tech Group, Inc. 2021. All rights reserved.

4 Cybersecurity

4.1 Critical Controls for a Security Framework

Having a security framework for adoption by businesses, would facilitate forward movement to compliancy, by knowing what security controls are necessary to purchase a Cyber Insurance policy from any carrier. Once a business requests insurance, that business could validate the framework was in place, or the business could make the necessary changes in their own security framework and state that those critical controls were active. This would be validated by an outside auditing firm's assessment, and the policy would then be placed in force. Some of these include the following:

MFA

Multi-factor Authentication (MFA) is quite simple to invoke, and many organizations are focusing more than ever on creating a smooth user experience for their employees (NIST, 2021). MFA is sometimes referred to two-factor authentication (2FA), it is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account; something you know – your password; and a generated 6-digit token that is generated by an authentication app on a smartphone that is tied to what you are logging into – something you have. Also, this would include biometrics like your registered fingerprint or iris scan (NIST, 2021).

VPN

Virtual Private Network (VPN) is a protected private tool for remote workers to log into the network, from any location with public Internet service. VPNs encrypt internet traffic and are secure for working with sensitive information; safely (Cisco, 2021). Remote workers are a risk to corporate data, according to the Identity Management Institute, a 2018 survey of CIOs reported they suspected their mobile workers had been hacked or were the cause of security problems. Only 46% could be "confident" their

© Company 2021. All rights reserved

remote employees used VPNs to increase security when connected to company networks (IMI, 2021).

Employee Cybersecurity Training

Insulating sensitive business information goes beyond strong passwords. According to MediaPro's third annual State of Privacy and Security Awareness Report, financial firms' employees performed the worst regarding cybersecurity awareness out of the seven industries evaluated. For the financial sector, 85% of workers lacked the knowledge around cybersecurity and data privacy. A comprehensive security awareness program sets clear cybersecurity expectations for all employees and educates users about how to recognize attack vectors (Align, 2021).

Critical Patching

In technology terms, patches are additional code to replace logic flaws existing in current software and operating systems. Consumers have the same obligation to have the fix applied, just as business does. When a patch is necessary to prevent unauthorized circumvention of a security control, the scope grows from quality control to include risk management (GIAC, 2021). Many organizations have regulatory and legal obligations to implement security updates in a timely manner. For some of these organizations, non-compliance with patching can have a huge impact on their ability to conduct business (GIAC, 2021). Having a patch management policy and needed maintenance windows to perform the installing of patches, is part of the security framework to protect the business and its data from attack.

Email (Incoming and Outgoing) Scanned for Malicious Attachments and Links

Email scanning automatically reviews every email message for viruses, malware, and spam. Email scanning also evaluates links and attachments for possible malicious attacks, and looks for suspicious addresses, domains and other signs of email spoofing often used in an impersonation attack (Mimecast, 2021). Email scanning technology is deployed both at the email perimeter and inside it. Scanning works automatically to look for infected attachments and URLs that seem suspicious, both for emails coming

© K2 Tech Group, Inc. 2021. All rights reserved.

into the business and internally (Mimecast, 2021). The scanning will halt a spam campaign attack, a phishing attack, and other malicious files such as ransomware, from affecting daily operations for business, cause loss of revenue, loss of data and loss of reputation.

Email scanning of outgoing messages is also important to validate that each outgoing message is free from any malicious file or message from a device that has been compromised but has not been discovered as being so. Again, this is important so to maintain security framework within, and to protect the recipients of business messages who may not have the same level of protection.

ALL NETWORK DEVICES PROTECTED WITH ANTI-VIRUS, ANTI-MALWARE OR ENDPOINT PROTECTION SOFTWARE

"Viruses, worms and Trojans, each of which has some unique characteristics, are starting to all blend together in people's perceptions as well as the way the behave. A virus can use worm-like logic to spread and install a Trojan horse type program. The distinctions are also mostly lost on the IT professional trying to keep this software from impacting their network and end nodes. Malware has been getting much more prevalent and virulent, even though programs that counteract these undesirable applications have been getting better and better (SANs, 2021)". Malware was once on a primary threat vector of diskettes, and the protection was a one-time issue, now the protection must be installed and continually running in the background, scanning of static files also need to be scanned for infections, and must be in real-time. Up-to-date virus signatures need to stay updated, most of the malware one will see in an inbox will have been released in the last 12 months (SANs, 2021). Compliance is spotty at best. One cannot keep up-to-date manually, all major anti-virus (AV) vendors have options that allow their applications to periodically check for new AV strings and automatically install them on the desktop or server. File server AV applications also perform the same AV activities as desktop; however, the file server apps also monitor Resource Utilization, heavy processor usage, having enough free RAM on the server is key to

© Company 2021. All rights reserved

keeping false positives from triggering a quarantine of a file, that may not be infected.

Viruses, worms, Trojans and Malware are here to stay, while malware keeps on getting more sophisticated and more prevalent, the tools and methods to deal with it keep on advancing. It is incumbent on the security administrator to keep on getting the education that they need to stay abreast of the current technologies at their disposal. While we know from experience that the next big outbreak of malware might use a method and vector that hasn't even been realized as yet, that are many actions that can be taken that can lessen the on-going background noise of unknown viruses and vectors (SANs, 2021).

CRITICAL DATA IS BACKED UP

All computer data needs to be backed up, from consumers to professional information technology of corporate, and small businesses operations. From desktops and laptops to servers and even mobile devices, all must be protected from loss or corruption. Recovery of lost or ransomware encrypted data, backups are the most valuable consideration for business continuity. The 3 – 2 – 1 – 1 – 0 is the newest rule in following the need for different stored recovery sources.

- 3 – 1 backup to the cloud, 2 off-site backups
- 2 – Storage on 2 different media
- 1 - Cloud Backup (Immutable)
- 1 – 1 Copy off-line
- 0 – Verified backup without errors (tested)

Recent expansion in high-speed internet access and cloud storage has changed data backups as a better guard against any worst-case scenario. Having these backups in the cloud, and in Write Once – Read Many (WORM) (Immutable) configurations and secured with the business's administrative password with MFA, is a safeguard against malware and ransomware infections. Having spinning hard drives that are approaching the mean-time-to-failure of operation (5 years) will test the worst-case scenarios, outside of a malware attack or a hard drive failure. Removing this scenario is to replace spinning hard drives with solid-state device hard drives (SSD), no moving

© K2 Tech Group, Inc. 2021. All rights reserved.

parts, no read/write arms or the need for a spinning platter. Read/writing to/from these devices also increases the seek and writing times which increases throughput of the node.

© Company 2021. All rights reserved

5 Summary

5.1 Closing

Having a 3rd party auditing firm assessing and verifying the Cybersecurity Insurance Carrier's requirements that are in-place for the potential policy owner's IT infrastructure, before issuance of a policy is key to having a policy in-place; having verified that those requirements are active at the potential customers location, prior to the policy being purchased. Any time after a Cybersecurity incident verifying compliance with the Cyber insurance policy is too late for both the insurance carrier and the policy holder. Asking for a self-assessment from the customer prior to issuance of a policy seems self-serving, and without having to have any real compliance adherence. It is recommended, and foreseen in the near future, that insurance carriers will be at the forefront of compliance adherence, prior to any government entity becoming involved.

© K2 Tech Group, Inc. 2021. All rights reserved.