ManageEngine
AD360

HANDBOOK

Cyber insurance decoded

Security controls that help reduce risks and cyber insurance premiums

www.manageengine.com/active-directory-360/

Index

Introduction

Are the cybersecurity practices you have adopted good enough to protect your organization's data? Even after studying people, processes, and technology for decades, this question haunts security leaders at organizations all over the world. Despite the efforts, intruders still infiltrate the security controls and disrupt the business processes. The loss, compromise, or theft of electronic data negatively impact businesses and they are liable for damages stemming from the theft of third-party data as well. Cyber insurance is important to protect organizations against the risk of cyber events, including those associated with terrorism.

In this e-book we highlight critical security settings that help your organization meet the minimum controls specified by underwriters. Meeting these basic controls help gain attractive insurance premiums and improve the cyber hygiene of your work environment.

What is cyber insurance?

Cybersecurity insurance, also called cyber liability insurance or cyber insurance, is a contract that can be purchased to help reduce the financial risks associated with doing business online in exchange for a monthly or quarterly fee. Cyber insurance has its origin from errors and omissions (E&O) insurance, a form of insurance that protects against faults and defects in the services a company provides.

Who needs cyber insurance?

Organizations that create, store, and manage electronic data online, such as customer contacts, credit card numbers, and other personally identifiable information of customers, can benefit from cyber insurance. Since downtime related to cyber incidents can cause a loss in sales and customers, e-commerce businesses can also benefit from cyber insurance.

Do small businesses need cyber insurance?

According to the Verizon's DBIR, among the 5,258 confirmed data breaches, 263 were reported by small industries with 1-1,000 employees and 307 by large industries with more than 1,000 employees. We don't know how many small industries are in the remaining 4,688 data breaches. However, it is evident from this data that a data breach can happen to an organization of any size. It largely depends on the type of infrastructure an organization relies on, and the type of data they handle. The wiser move is getting cyber insurance if you are handling customer data and digital assets, like vlogs and e-books.

What is covered by cyber insurance?

Cyber insurance policies help cover the financial losses that result from cyber events and incidents. In addition, cyber-risk coverage helps with the costs associated with remediation, including payment for the legal assistance, investigators, crisis communicators, and customer credits or refunds. The expenditures typically include costs associated with the following:

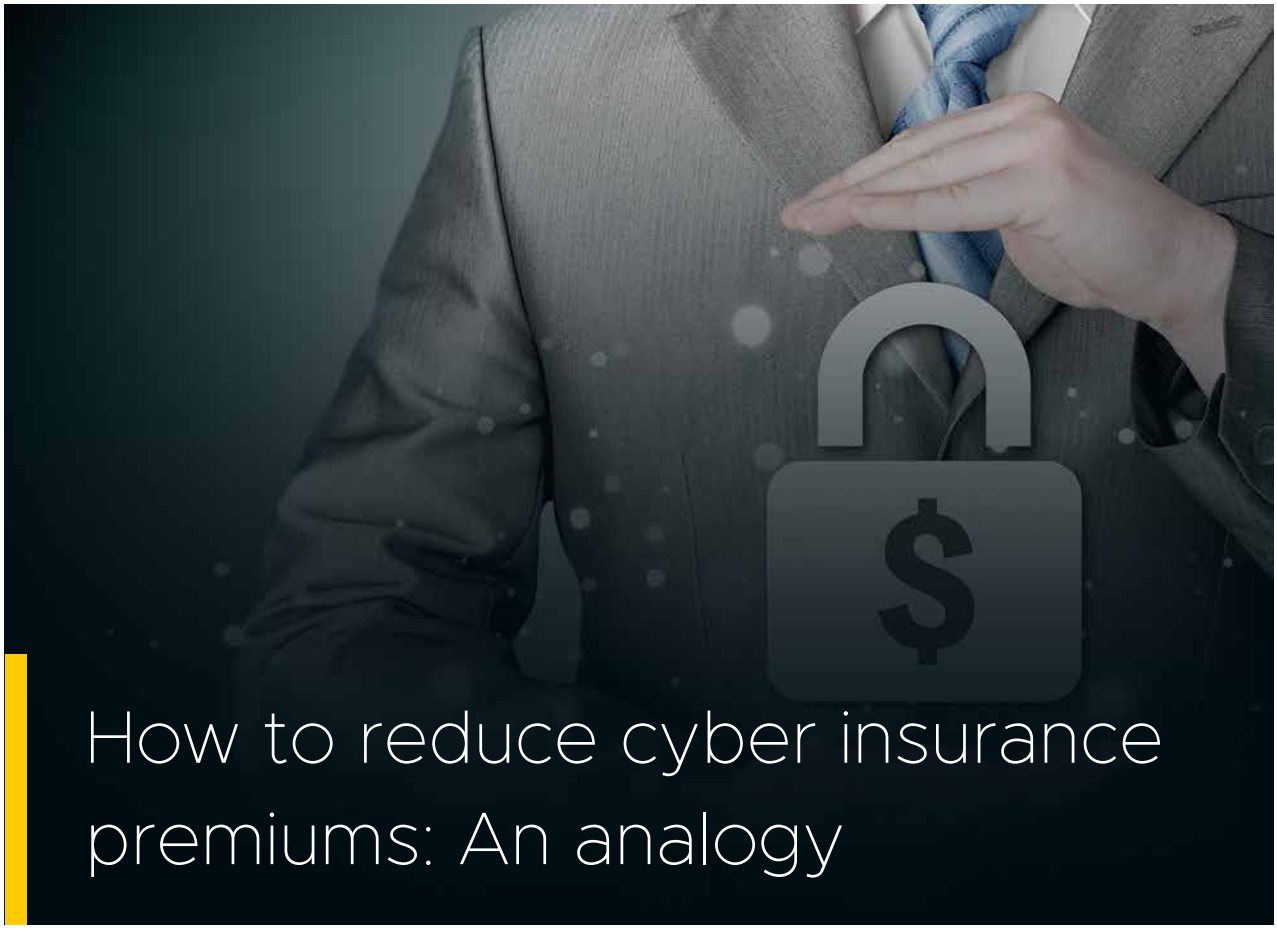
- Meeting extortion demands from a ransomware attack.
- Notifying customers when a security breach has occurred.
- Paying legal fees levied as a result of privacy violations.
- Hiring computer forensics experts to recover compromised data.
- Restoring identities of customers whose personally identifiable information (PII) was compromised.
- Recovering data that has been altered or stolen.
- Repairing or replacing damaged or compromised computer systems.

Depending on the type of policy and policy provider, some insurers are beginning to offer policies that cover third-party liability losses as well.

What is not covered by cyber insurance?

Many cybersecurity policies exclude preventable security issues caused by humans, such as poor configuration management, or the careless mishandling of digital assets. Other issues excluded by cybersecurity policies include the following:

- Preexisting or prior breaches or cyber events, such as incidents that occurred before the policy was purchased
- Cyber events initiated and caused by employees or insiders
- Infrastructure failures not caused by a purposeful cyber attack
- Failure to correct a known vulnerability
- The cost to improve technology systems, including security hardening in systems or applications



How to reduce cyber insurance premiums: An analogy

Cyber insurances are similar to health insurances. If you have a current health condition at the time of purchasing the insurance, or any ill habit that might affect your health, then you might be ineligible to get insurance or your insurance premium will be high. The insurance providers expect the insurance buyers to be healthy, without any major health complications, and to follow healthy life habits.

Similarly, the cyber insurance underwriters expect some minimum controls to be implemented in your organization. End-to-end encryption, multi-factor authentication (MFA), and compliance with regulatory policies are some examples. Depending on the security measures taken by the organization, the insurance premiums vary. For example, a home with burglar alarms and fire detection systems typically receives a more affordable premium than the home without them. Not that the insurance company expects a home will be robbed, but the underwriters expect some minimum controls to be in place in case of emergencies.

Minimum controls that can be implemented

In this section we have consolidated a few security controls that help thwart known cyberattacks and describe how AD360, ManageEngine's IAM solution help you implement them efficiently.

Multi-factor authentication

According to Verizon, 61% of known security breaches involved credentials. Defend your organization from password-based attacks, like brute-force attack, password spray, and dictionary attacks using MFA. Whether for an application or an endpoint, it is necessary to enable MFA to help protect your IT infrastructure.

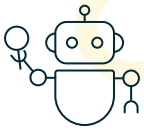
How we help: With ManageEngine AD360, you can configure MFA for on-premises and cloud applications, and endpoints in your network. It can secure both local and remote login attempts to server and user machines, prevent credential-based threats, and help meet compliance mandates.

Password policies

Weak passwords allow the hackers into a network. According to a recent survey, 68% of people use the same password for different accounts across different platforms. This means that once a user account is compromised, all the accounts with the same password will also fall victim. In these cases, hackers just login rather than break in.

How we help: AD360's Password Policy Enforcer comes with some unique password restrictions that cannot be found in native Active Directory (AD) and cloud applications. You can configure policies that can be applied to specific organizational units, reject passwords with a consecutive repetition of the same character, restrict the use of palindromes and dictionary words as passwords, specify the number of times a particular character can be used, and more.

User behavior analytics



Perusing the audit logs and detecting threats is nearly impossible. A tool with user behavior analytics (UBA) capability will analyze the audit logs and notify you when a malicious or suspicious activity takes place.

How we help: AD360 alerts you when a server is accessed during non-business hours, a dormant account becomes active, an unusual number of user management activity is detected, someone attempts to delete data, an unusual process runs in the machine, and more.

Change auditing

Auditing is both necessary and mandatory when it comes to an organization's security. It serves both as a reactive and proactive measure to respond to threats. The audit logs help to analyze the attack surface and a capable tool will alert IT admins when things look suspicious.

How we help: With AD360's UBA-driven change auditor, audit, AD, file servers, Windows servers, and Windows workstations in real time. With this one tool, you can also audit a hybrid Exchange setup, Azure AD, Microsoft Teams, and other major Microsoft 365 services.

Email monitoring

Phishing has been the top technique used in successful security breaches by hackers in the past three years. Therefore, it is important to monitor emails as well as servers and user machines.

How we help: With AD360's content search capability, you can identify emails with PII, unusually large attachments, suspicious links, and other specified keywords that might indicate the presence of dubious links. Monitoring incoming and outgoing email traffic helps you detect bulk emails which are usually a sign of a phishing attack.

Backup and recovery

According to a recent research, ransomware has doubled in frequency since 2021. In this attack, the threat actors exfiltrate critical data, encrypt it, and threaten the organization to expose the data publicly in order to collect a ransom. If organizations don't have a proper backup and recovery solution in place, their reputation and finances might suffer.

How we help: AD360's backup and recovery module helps take incremental backups of on-premises AD, Azure AD, Microsoft Office 365, Google workspace, and on-premises Exchange. In case of loss of data due to a ransomware attack or human error, restore all files, folders, user attributes, AD objects, mailboxes, calendars, contacts, and every other entity in your workspace in a single click.

Role-based access control

Privilege abuse is the most common action taken by the hackers involved in financial frauds and espionage. A top recommended mitigation technique to prevent privilege abuse is using role-based access controls. With this strategy, technicians are given access only to the modules they need to work on, instead of full admin privileges.

How we help: AD360 allows you to create custom help desk roles that can be assigned to technicians without providing admin privileges. Custom roles can be created for on-premises AD and Microsoft 365 using AD360, and there is no restriction on the number roles that can be created.

Compliance

Complying with industrial mandates is both mandatory and necessary for organizational security. Non-compliance affects the organization's reputation as well as its finances.

How we help: AD360's granular audit reports and management capabilities help to comply with SOX, HIPAA, GDPR, PCI DSS, GLBA, FISMA, ISO 27001 and more.

Conclusion

The list of minimum controls required does not remain the same all the time. After every major security breach, insurance underwriters keep adding more security controls to the list. At the time of purchase, the buyers are expected to have implemented them

Insurance underwriters often insist on anti-phishing controls, data encryption, network segmentation, and other basic network hygiene practices in order for organizations to receive a decent cost for their policies. Although cyber insurance is a new industry, with the continuing shift towards cloud services, obtaining cyber insurance will soon be unavoidable.