IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

Cyber Insurance and ITDR: A Perfect Match?

James (Jim) Doggett

James (Jim) Doggett
Chief Information Security Officer
Semperis

Biography

James (Jim) Doggett is the Chief Information Security Officer at security specialists, Semperis (https://www.semperis.com). With more than 35 years of experience leading cybersecurity and risk programs at global organizations, James is a high energy leader focused on embedding risk management, security, and compliance into the business fabric to efficiently manage risks.

He is a retired partner from EY where he spent 27 years helping clients through financial audits and building and sustaining security, risk and controls. Previously, he served as global leader of Information Risk and Resiliency for the Treasury and Security Services division of JP Morgan, Chief Security Officer (CISO) and Chief Technology Risk Officer for Kaiser Permanente, and Chief Technology Risk Officer and CISO for AIG. Subsequently, helped start up Panaseer in building the first continuous controls monitoring platform (remain as Board Advisor).

Jim shares his insights in Semperis company blogs at https://www.semperis.com/blog/

Keywords Cyber insurance, Identity Threat Detection and Response (ITDR), Active Directory, Backup, Disaster Recovery (DR), Threat detection, Identity security
Paper type Research

Abstract

In a world where cyber threats are varied (and constantly changing), cyber insurance can protect organizations from losses due to security incidents. As well as minimizing business disruption and providing financial protection during an incident, cyber insurance may help with any legal and regulatory actions after an incident. But with organizations struggling with the escalating cost of cyber insurance, now is the time for every business to demonstrate a strong posture when it comes Identity Threat Detection and Response, explains the author of this article.

Introduction

Given the rise of ransomware, breaches, and cyberattacks – and the accompanying risk of reputational damage, compliance violations, penalties, and Intellectual Property (IP) loss – many organizations have begun looking to cyber insurance to protect themselves from the financial damage associated with an attack. Others are struggling with the escalating cost of cyber insurance and the need to demonstrate a strong security posture.

However, the potentially exorbitant cost of such claims and the complexity of safeguarding increasingly complex digital ecosystems means that such coverage can be pricey. Plus, qualifying for a policy isn't a given. Even with coverage, organizations that suffer an attack can find that an oversight in their security stance leaves them with a rejected claim. Therefore, relying solely on cyber insurance to protect your IP, customer data, and public reputation is a risky bet.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Fortunately, many requirements for cyber insurance coverage overlap with best practices for effective identity threat detection and response (ITDR). Therefore, to increase compliance with insurer requirements such as implementing steps to protect Tier 0 assets like Active Directory (AD) – while at the same time, decrease the likelihood that you will need to call on that coverage.

The challenge of meeting cyber insurance requirements

The rapid rise of cyberattacks[1] targeting companies of nearly every size and industry are alarming. A successful breach can lead to a shutdown of company operations, loss of reputation, and significant fines[2], in addition to financial losses tied directly to the attack.

Cyber insurance strives to help organizations offset financial loss in the event of a cyberattack or breach. Although not a complete list, these losses typically relate to the following:

- System damages
- Business interruption
- Privacy, penalties, and claims
- Contractual breaches
- Data recovery
- Professional expertise fees

However, to qualify for coverage (or reduce your premium), organizations must meet a growing list of requirements. Rates, retention periods, and other control measures depend on your risk profile. Even if you qualify for and purchase a policy, if you fail to maintain


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

strong defenses, your provider might balk at covering a claim if – or when – an incident occurs.

A single click or minor misconfiguration can lead to a major breach – and if your organization fails to meet the security requirements defined by the insurance provider, your policy could be in jeopardy. Clearly, cyber insurance is not a fail-safe for any loss or for any reason.

Aside from a nearly ubiquitous demand for multifactor authentication (MFA), eligibility for coverage and payment often includes the following requirements:

- **Backup and disaster recovery** – regularly back up data and verify that it is retrievable in case of an attack.
- **Endpoint detection and response (EDR)** – install antivirus solutions to protect endpoints against malware, viruses, and other attacks.
- **Identity and access management (IAM)** – authorize and authenticate users and maintain least privilege policies to make access by attackers more difficult.
- **Privileged access management (PAM)** – monitor privileged accounts to detect suspicious behavior and quickly identify compromised accounts.
- **Patch management** – consistently implement patches and updates.

What about Active Directory (AD) – your most important Tier 0 asset?

Identity is the new security perimeter, and for most organizations, AD is at its heart. Due to AD's extensive control and capabilities over your other digital assets (for example, your critical applications), cybercriminals often target it as their final goal.

Cyberattacks on AD aim to give attackers access to privileges that enable them to plan and execute further attacks. Protecting AD is a vital aspect of maintaining a strong security stance and mitigating risk. Unfortunately, AD, despite having much information about an entire organization, is often not the primary focus when it comes to strengthening the organization's security posture.

Furthermore, many key applications depend on AD for login functions. For many companies, when AD stops operating, those applications become unusable, too.

In addition, environments that include both on-premises AD and Azure AD complicate ITDR. Despite their common name, these two identity solutions have very different security models[3].

Why an effective AD security approach benefits cyber insurance

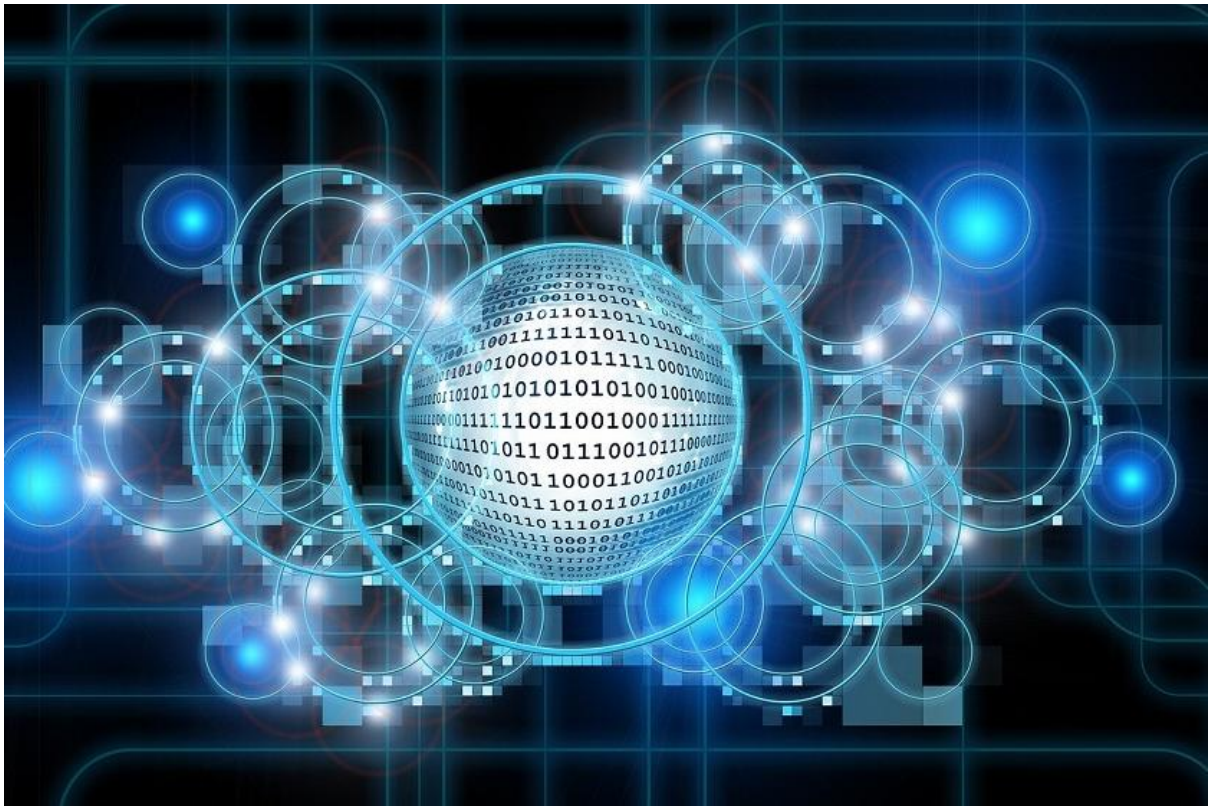
Security always needs to be a continuous process. Both preventive and corrective solutions are important – you must choose the right products to mitigate or minimize the security risks before, during, and after an attack.

Endpoint Detection and Response (EDR), Multi-Factor Authentication (MFA), and other security solutions are important but are not AD-centric and do not protect AD across this entire attack lifecycle. When an attacker gets past those measures, AD is vulnerable – unless you have AD-specific identity protection in place.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Several of the previously mentioned cyber insurance requirements *are* part of an effective AD security approach. These include AD-aware backups, careful adherence to least privilege principles, and the ability to quickly detect and remediate suspicious privilege escalations. We'll explore them further to explain why.



Backups

Backups are a minimum requirement of many cyber insurance providers. The goal is to get back online quickly in the event of a ransomware or other attack. But what if your backup carries the same malicious payload that infected your environment in the first place?

If your domain controllers are already infected when backups are made, you face a lose-lose choice: Restore an infected backup and start the whole cycle over again or lose time and data digging through backups until you find one taken before malware introduction.

Maintaining and regularly testing reliable, malware-free AD-aware backups is one of the most effective risk-mitigation steps you can take. A dedicated AD backup and recovery plan, separated from OS backup and recovery, can literally save the day when attackers lock down your systems.

Gartner recommends[4] a dedicated AD backup and recovery solution to minimize the impacts of a cyberattack, noting that tools such as Semperis Active Directory Forest Recovery (ADFR)[5] "offer a more complete backup and recovery platform for Active Directory than those found in the Active Directory modules included in most enterprise backup software." ADFR also offers a smaller backup footprint: just over 700 MB, compared with 175 GB for system state backups and 200+ GB for bare metal backups.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Identity and access management (IAM) and Privileged access management (PAM)

Gartner notes[6], "Organizations have spent considerable effort improving IAM capabilities, but much of it has been focused on technology to improve user authentication, which actually increases the attack surface for a foundational part of the cybersecurity infrastructure … ITDR tools can help protect identity systems, detect when they are compromised and enable efficient remediation."

Applying least privilege, role-based access control (RBAC), and monitoring of high-privilege accounts is vital to AD security. Especially in large organizations, the overwhelming amount of data generated in security logs can make it difficult to spot gaps caused by human error or configuration creep – gaps that attackers can use to escalate privileges and wreak havoc. The ability to automatically detect suspicious activity when and where it occurs, rather than depending solely on log monitoring, and roll back suspect changes can help prevent the lateral movement that attackers favor.

Semperis Directory Services Protector (DSP)[7] helps you prevent attackers from gaining access to AD by checking for security indicators of exposure or compromise – even those that bypass security logs. DSP can also automatically remediate changes made until you can review and approve them. DSP provides continuous monitoring, which is critical to maintaining a secure environment. DSP provides an end-to-end security coverage allowing you to quickly remediate vulnerabilities discovered in AD (automatically or via an alert to your SOC).

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Meeting cyber insurance requirements while protecting AD

Even in a controlled, well-managed environment with a solid secure foundation, evolving cyberattacks are a continuous threat. Cyber insurance can help you recover financially but cannot offset reputational damage or data loss.

Semperis DSP and Active Directory Forest Recovery (ADFR) provide strong protection for AD, strengthening your organization's overall security stance – something cyber insurers prize. Semperis also offers a free AD security assessment tool, Purple Knight[8], which you can use to identify potential AD security gaps so that you can remediate them before applying for cyber insurance.

By taking a proactive approach to AD security, you can decrease risk and increase your overall security stance – a win-win, regardless of whether you maintain cyber insurance.

Reference

1 Brooks, C. (21 January 2022), Cybersecurity in 2022 - A Fresh Look at Some Very Alarming Stats. Forbes. . Available at: https://www.forbes.com/sites/chuckbrooks/2022/01/21/cybersecurity-in-2022--a-fresh-look-at-some-very-alarming-stats/?sh=66104e3d6b61

2 Pipeline and Hazardous Materials Safety Administration, PHMSA Issues Proposed Civil Penalty of Nearly $1 Million to Colonial Pipeline Company for Control Room Management Failures (5 May 2022). United States Department of Transportation. Available at: https://www.phmsa.dot.gov/news/phmsa-issues-proposed-civil-penalty-nearly-1-million-colonial-pipeline-company-control-room

3 Grillenmeier, G. (4 August 2022), Securing Hybrid identity. Semperis. Available at: https://www.semperis.com/blog/securing-hybrid-identity/

4 Simpson, N. (21 September 2021), How to Protect Backup Systems From Ransomeware Attacks), Gartner Research. Available at: https://www.gartner.com/en/documents/4005993

5 Active Directory Forest Recovery. Semperis. Available at: https://www.semperis.com/adf-recovery/

6 Gartner Identifies Top Security and Risk Management Trends for 2022 (7 March 2022), Gartner. Available at: https://www.gartner.com/en/newsroom/press-releases/2022-03-07-gartner-identifies-top-security-and-risk-management-trends-for-2022

7 Directory Services Protector. Semperis. Available at: https://www.semperis.com/ds-protector/

8 Purple Knight. Semparis. https://www.purple-knight.com/