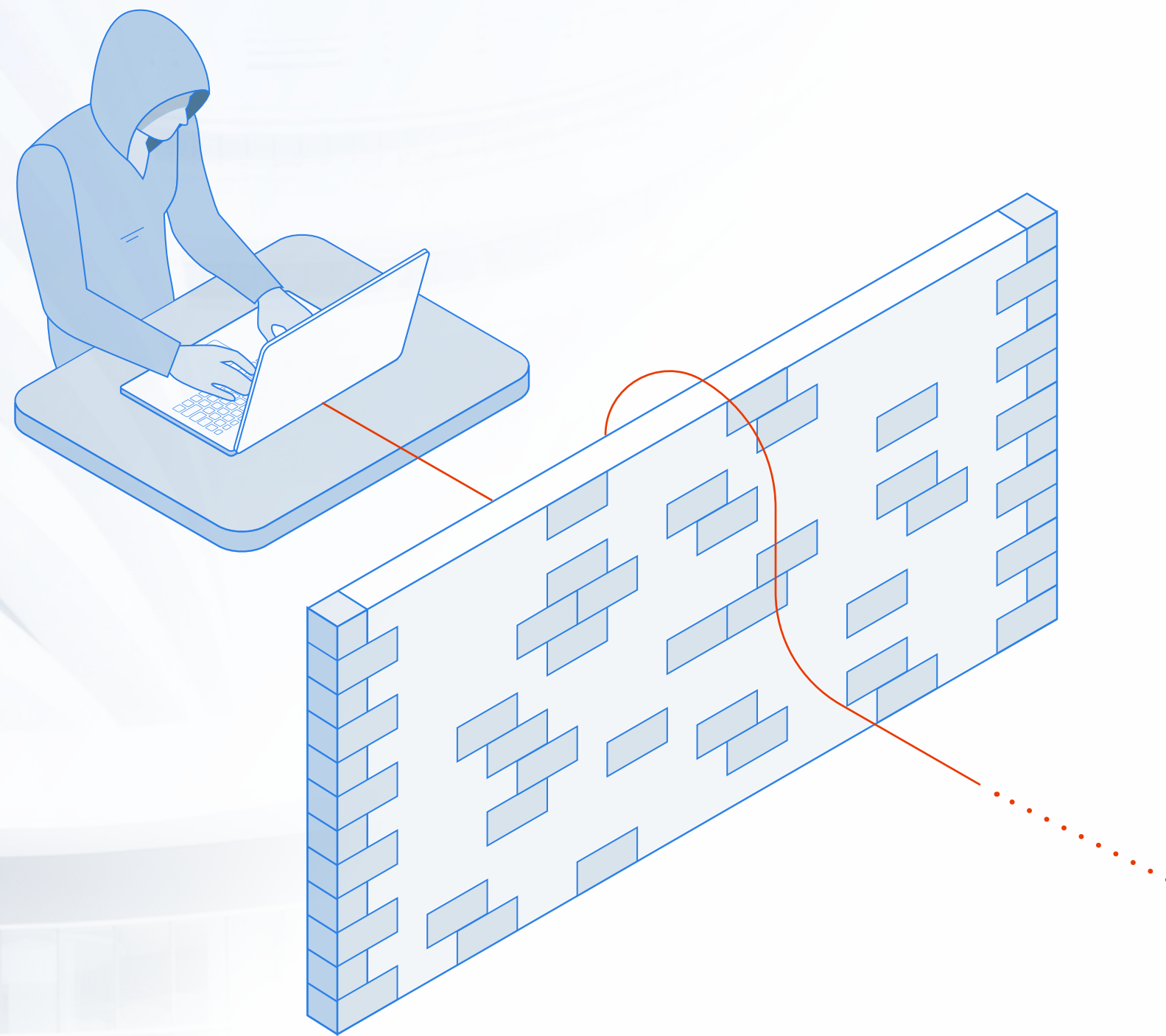




Episode 3

HOW TO CONVINC
YOUR C-SUITE THAT
**ACTIVE DIRECTORY
SECURITY MATTERS**





Years of (over)simplification have taught our whole industry that attacks begin outside an enterprise, fly through its networks and endpoints, and eventually reach (and often sabotage) their data and vital assets.

Unfortunately, this somewhat naive model has led senior management to ignore or neglect the security of the ubiquitous, all-powerful overseer that orchestrates literally everything in any given IT infrastructure: Active Directory (AD). As a consequence, it receives too little investment and brainwork from boards, and far too much attention from hackers.

This document aims at providing tangible arguments to security managers and CISO for convincing their Board of Directors that the defense of their Active Directory is paramount to the security of their business.





HIGH-LEVEL RISKS

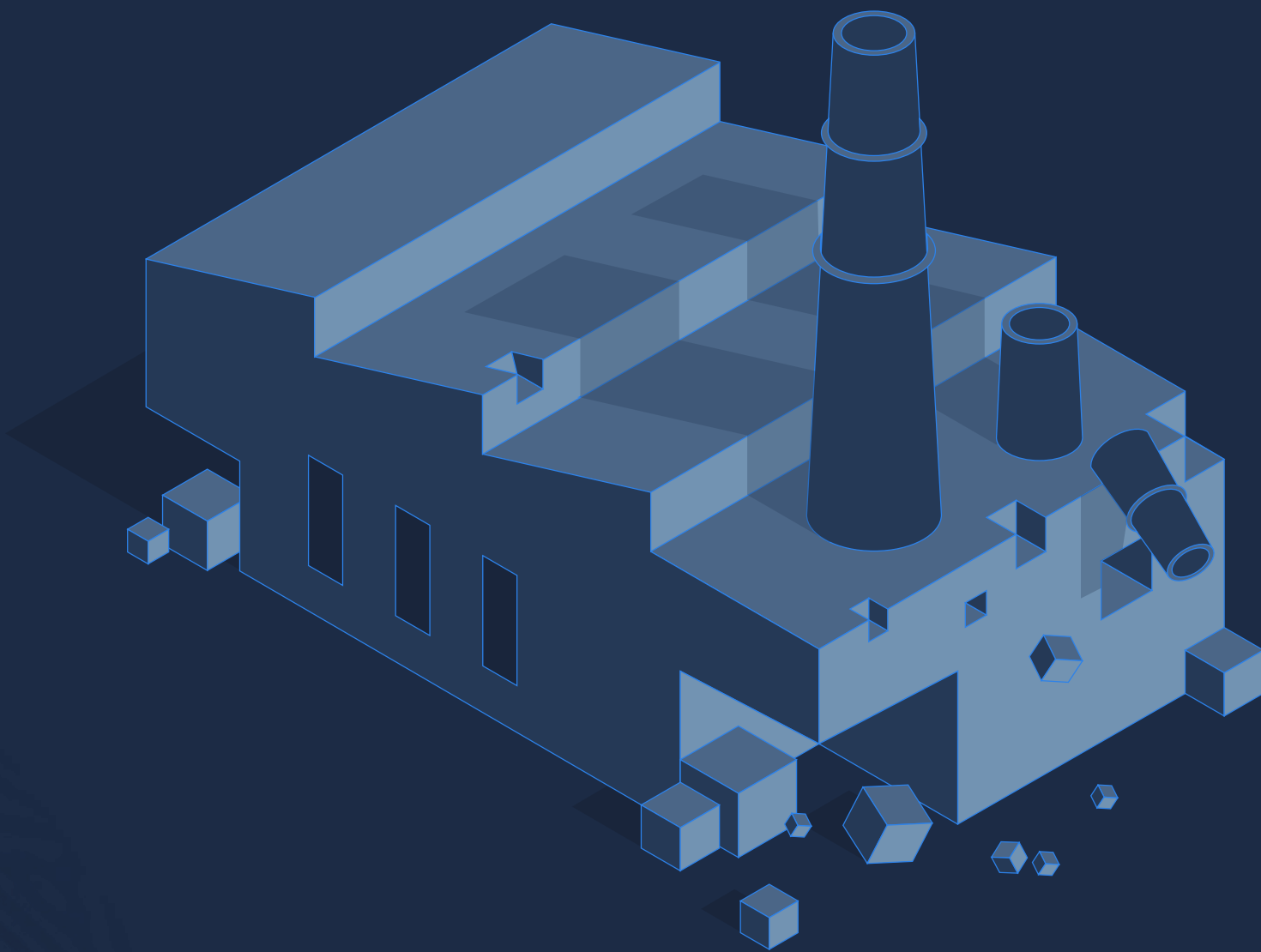
Being the global orchestrator of your IT infrastructure, Active Directory is, by design, a single point of failure. On the other hand, Active Directory forests are perpetually evolving, in tandem with the enterprises' organigrams, business architectures, and M&A activities. Thus Active Directory is also, by construction, a heterogeneous system whose security hygiene gets quite ugly quite quickly. That being said, what are the actual, corporate-level risks that result from this weak link's central position?

Business (Dis)Continuity

This is the most tangible threat Active Directory's insecurity poses to industries and enterprises. Halting factories, grounding planes, preventing employees from accessing their emails... Nullifying an organization's business capabilities is not a 007 scenario or just a nightmare for overanxious security professionals.

There are two ways hackers exploit Active Directory that lead to dramatic business disruptions:

- **Crippling Active Directory itself.** By undermining the very foundation of an organization's IT, attackers can prevent users and applications from logging in to their systems and accessing their required resources. And while this may seem a hit-and-run tactic, there are some well-documented – albeit poorly addressed – procedures for hackers to persist into their victim's AD even after a greenfield rebuild. Seek, destroy, repeat.



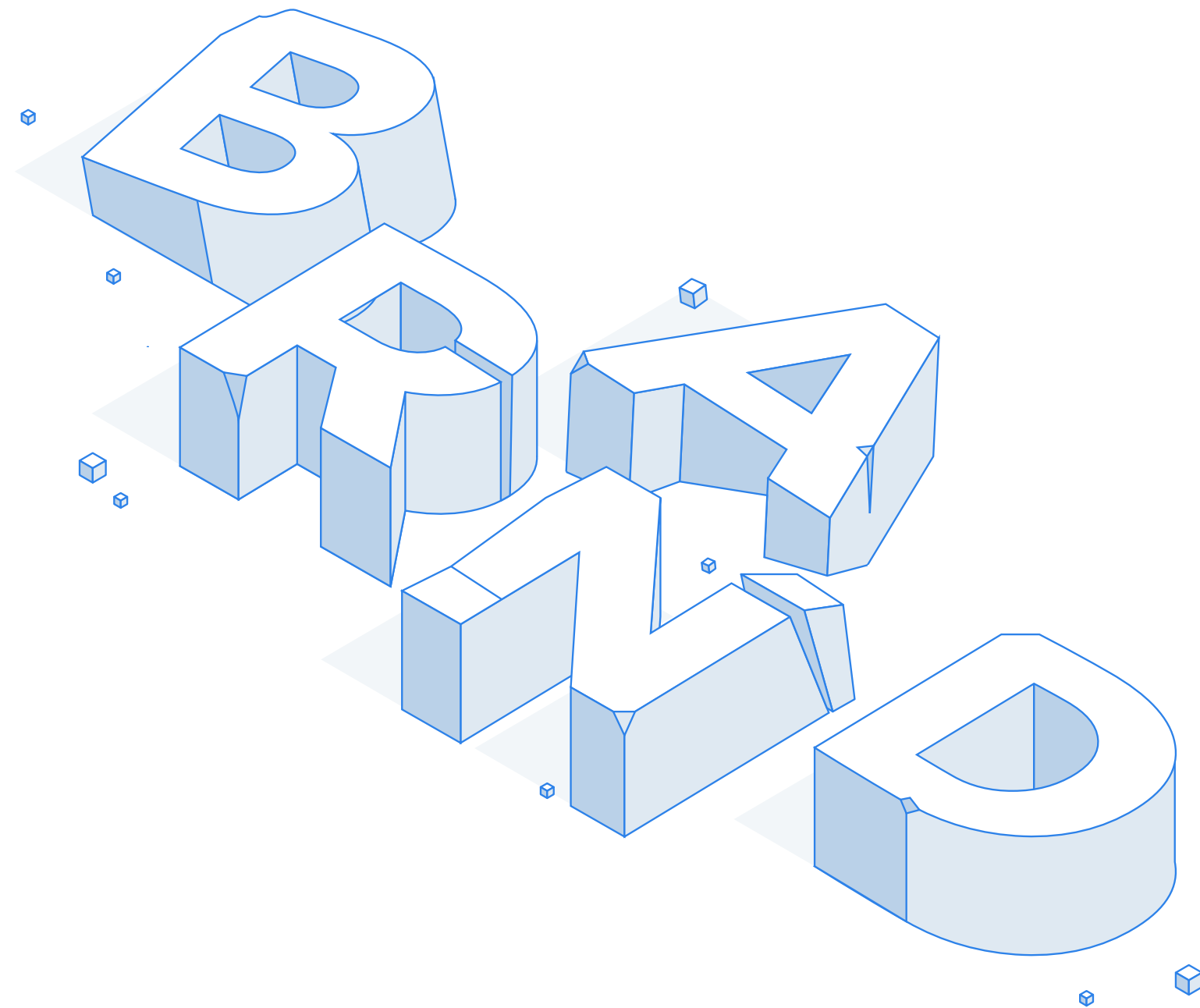


- **Using Active Directory as a transport for destructive malwares.** Destructive malware is not rocket science. Highly-sophisticated payloads such as Stuxnet are the exceptions, while today's consumer-level ransomwares are good enough to do the destruction job effectively. The only challenge in those attacks is distribution: getting these malwares installed on a sufficiently large number of endpoints so that recovery at scale becomes unrealistic. In this regard, exploiting Active Directory weaknesses is the only practical option for hackers to move laterally within the infrastructure. Every large-scale, infrastructure-wide attack that has crippled production capabilities in recent years has had an Active Directory exploit at its core.

Examples:

- **March 2018:** Norsk Hydro is forced to switch to manual operations after LockerGoga encrypts and disconnects systems that manage factory equipment. The incident has been described as disastrous by Hydro officials.
- **June 2017:** A NotPetya ransomware attack shuts down the port terminals of Danish shipping giant Maersk for two days, causing an estimated \$300 million in associated costs.
- **December 2017:** French company Schneider Electric is forced to shut down operations of a power plant in the Middle East after malware compromises its industrial control systems. Analysis by security researchers indicates that the attack was sponsored by a nation-state.
- **April 2011:** A coordinated attack on Sony's PlayStation Network shuts the service down for a month, leading to an estimated loss of \$171 million.





Brand Damage and Customer Trust

This is by far the most visible damage caused by cybercrime today. With personally identifiable information (PII) leaks making the headlines almost every week, the public reaction tends to become... tense.

In early 2016, a survey by The Economist Intelligence Unit asked 282 C-suite members about their concerns in cybersecurity: “our reputation with our customers” ranked an unequivocal first. This should not be a surprise considering the brand is the overarching umbrella of a company; brand damage has a ripple effect that impacts all its products and services. Moreover, public data breaches tend to be followed by years of customer and shareholder lawsuits.

Those events are widely publicized and recurrently damage a brand and its products.





Contrary to business disruption attacks, data breaches do not always require an Active Directory hack to be effective... only very often, depending on whether the hack requires deep intrusion into the infrastructure or not.

Examples:

- **September 2018:** SingHealth's infrastructure breach involves 1.5 million personal records, plus the prescription details of 160,000 patients, including those of Prime Minister Lee Hsien Loong.
- **November 2014:** Sony Pictures Entertainment is hacked, with the malware deleting data and the hackers posting online employees' personal information and unreleased films. An FBI investigation reveals North Korea was behind the attack.
- **March 2014:** Cybercriminals steal 40 million credit card numbers from Target, with an additional 70 million accounts compromised.





COMPETITIVE LOSS AND IP THEFT

In this digital, fast-paced, innovation-driven century, Intellectual Property is the blood and soul of enterprises. Having IP in the wild is not simply an embarrassment, it's a direct threat to the very existence of the organization.

In the tech industry at large, blueprints and products are designed months ahead of their public release, giving IP thieves a sufficient lead to preemptively close technical gaps and nullify competitive advantages. In critical national industries, IP thefts have geopolitical consequences no enterprise wants on its track record. Finally, the media and videogame industries are unfortunately now accustomed to seeing their AAA productions leaked into the wild before they reach theaters and shops.

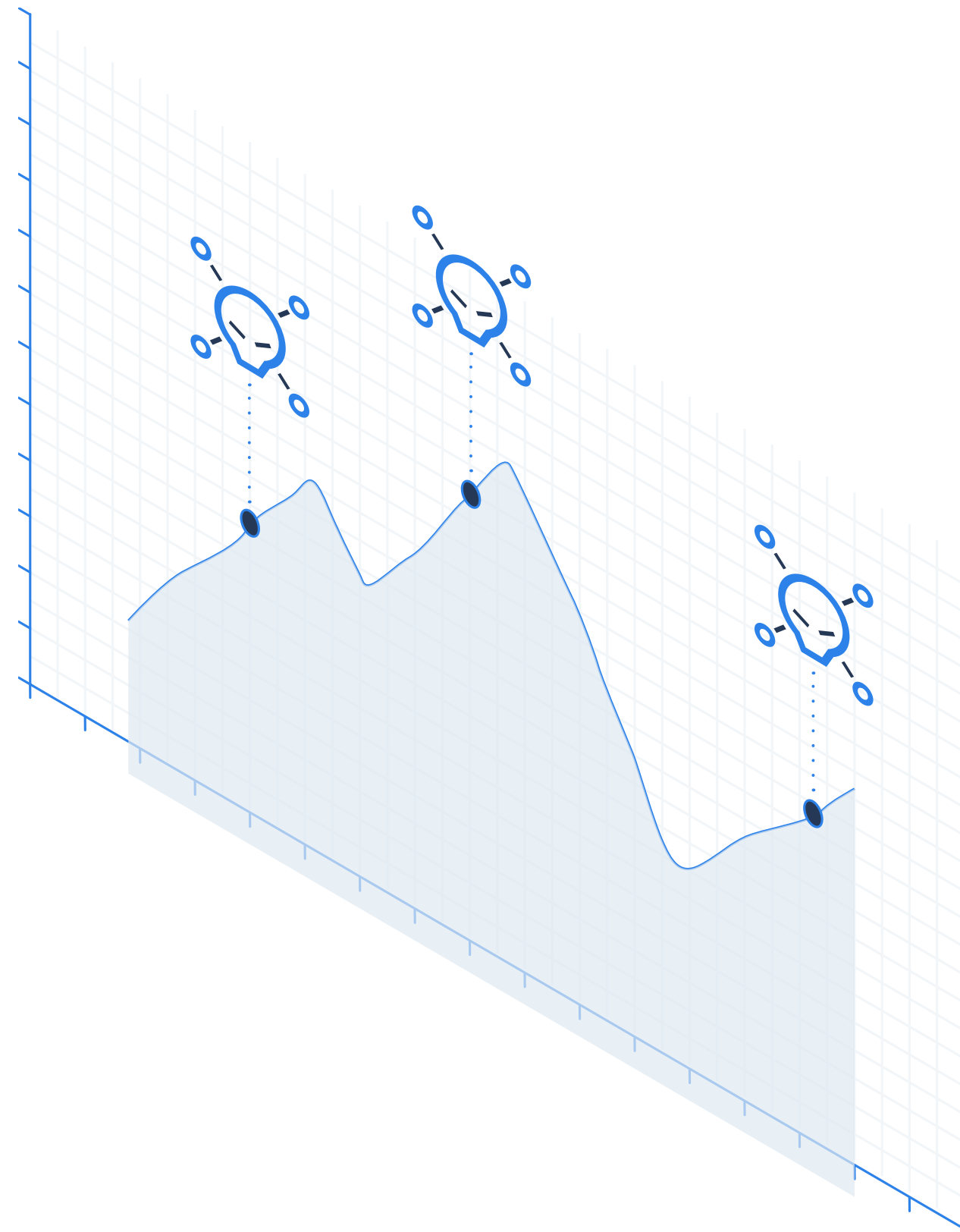
Exfiltrating these data stealthily remains the easiest, albeit not a trivial, part of a hacker's job. Their true challenge lies in accessing the data in the first place: after primo-infection, an attacker rarely has access to his/her targeted assets.

Hunting for the valuable data requires the ability to hop from system to system until proper access rights can be inherited or impersonated. And there is only one way to do so: exploiting Active Directory vulnerabilities.

Examples:

- **January 2010:** Operation Aurora is a series of attacks that targets dozens of tech organizations, including Google, Adobe, Juniper, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical.
- **November 2014:** Sony Pictures Entertainment is hacked, with the malware deleting data and the hackers posting online employees' personal information and unreleased films. An FBI investigation reveals North Korea was behind the attack.





(Cyber)Insider Trading

These cybercriminal activities are by nature difficult to quantify, but several recent empirical studies found strong correlations between drops in stock prices and breach announcements. Hacker groups involved in Cyber Insider Trading fall under two distinct categories:

- Hacker-traders steal non-public data to inform their trades, thereby gaining an unfair advantage in the free market. Notable cases involve massive theft of soon-to-be-disclosed earning reports (SEC case, see later) or early-stage indications of M&A projects at enterprises or investment banks.
- Traditional cybercriminals anticipate a drop in their victims' stock price after the disclosure of their attack, and thus increase their attack's return-on-investment by adding a trading component to it.





As for any other malware-driven cybercrime, exploiting Active Directory remains the only effective way for hackers to move within an organization's IT until they gain access to the data they are seeking.

Examples:

- **January 2019:** The U.S. Securities and Exchange Commission charges a group of hackers from the U.S., Russia, and Ukraine with the 2016 breach of the SEC's online corporate filing portal, exploited to execute trades based on non-public information.
- **December 2014:** FIN4 cybercriminal group is discovered hacking more than 100 companies, investment advisers, and law firms in search of market-moving information about deals, according to researchers at cybersecurity company FireEye.





▲ Direct Financial Losses and Stock Prices

Our industry now has a couple of decades of reference points on cyber extorsions, vandalism, and theft. This sad history has at least one good facet: the direct, immediate financial cost of attacks is now a well-documented field of research. There are four direct, immediate ways enterprises and shareholders lose money because of a cyber incident:

- **Sudden stock price drops**
- **Legal penalties and charges**
- **Money heists**
- **IT remediation costs**

As explained earlier, no large-scale attack on an IT infrastructure would succeed without exploiting, at some point, a few Active Directory weaknesses. All these costs are therefore linked to the insecurity of this critical infrastructure.



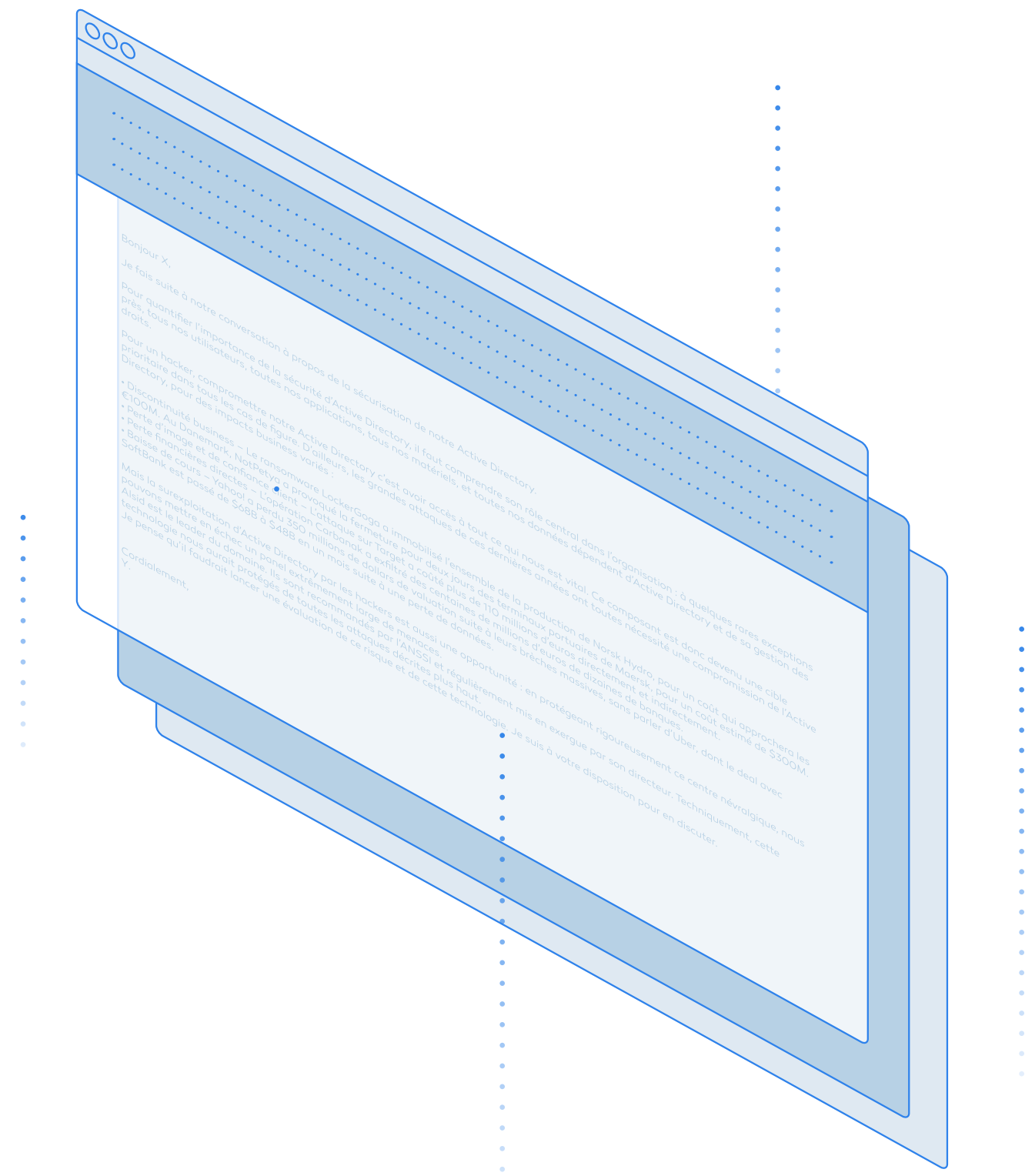


The IT remediation costs themselves can grow exponentially according to the post-incident state of Active Directory itself: if it's entirely compromised – which is often the case – then the remediation truly is a greenfield rebuild. This painful process usually mobilizes dozens, sometimes hundreds, of employees and specialized contractors who refactor the entirety of the architecture during nights and weekends. And that comes at a great cost.

Examples:

- **January 2018:** A Japanese-based cryptocurrency exchange reveals that it lost \$530 million worth of the cryptocurrency NEM in a hack, in what amounts to possibly the largest cryptocurrency heist of all time.
- **December 2017:** SoftBank acquires roughly 15% of Uber. The deal valued Uber at about \$48 billion, after Uber suffered (and horribly managed) a massive customer data breach. A month before the breach, Uber's valuation peaked at \$68 billion. Not all of this 30% drop is attributable to the breach, but analysts see it being a significant factor.
- **June 2017:** Verizon completes the acquisition of Yahoo!'s operating business for \$4.48 billion, after the latter suffered two highly publicized breaches that knocked an estimated \$350 million off its sale price.
- **September 2014:** An attack on the POS systems of Home Depot exposes the credit/debit card information of 56 million customers. In March 2016, the company agrees to pay \$13 million to reimburse shoppers for out-of-pocket losses, and to spend at least \$6.5 million to fund 1.5 years of cardholder identity protection services. Overall, the company allocates \$161 million of pre-tax expenses to the breach.
- **December 2013:** Target suffers a massive breach of its POS system, leading to the theft of credit/debit card information and/or contact information of up to 110 million people. Target's CIO resigns in March 2014, and its CEO resigns in May of that same year. The company estimates the cost of the breach at \$162 million.





Email Template

This email template aims at providing CxOs with a summary of the Active Directory insecurity issue.





○○○

Bonjour X,

Je fais suite à notre conversation à propos de la sécurisation de notre Active Directory.

Pour quantifier l'importance de la sécurité d'Active Directory, il faut comprendre son rôle central dans l'organisation : à quelques rares exceptions près, tous nos utilisateurs, toutes nos applications, tous nos matériels, et toutes nos données dépendent d'Active Directory et de sa gestion des droits.

Pour un hacker, compromettre notre Active Directory c'est avoir accès à tout ce qui nous est vital. Ce composant est donc devenu une cible prioritaire dans tous les cas de figure. D'ailleurs, les grandes attaques de ces dernières années ont toutes nécessité une compromission de l'Active Directory, pour des impacts business variés :

- Discontinuité business – Le ransomware LockerGoga a immobilisé l'ensemble de la production de Norsk Hydro, pour un coût qui approchera les €100M. Au Danemark, NotPetya a provoqué la fermeture pour deux jours des terminaux portuaires de Maersk, pour un coût estimé de \$300M.
- Perte d'image et de confiance client – L'attaque sur Target a coûté plus de 110 millions d'euros directement et indirectement.
- Perte financières directes – L'opération Carbanak a exfiltré des centaines de millions d'euros de dizaines de banques.
- Baisse de cours – Yahoo! a perdu 350 millions de dollars de valuation suite à leurs brèches massives, sans parler d'Uber, dont le deal avec SoftBank est passé de \$68B à \$48B en un mois suite à une perte de données.

Mais la surexploitation d'Active Directory par les hackers est aussi une opportunité : en protégeant rigoureusement ce centre névralgique, nous pouvons mettre en échec un panel extrêmement large de menaces.

Alsid est le leader du domaine. Ils sont recommandés par l'ANSSI et régulièrement mis en exergue par son directeur. Techniquement, cette technologie nous aurait protégés de toutes les attaques décrites plus haut.

Je pense qu'il faudrait lancer une évaluation de ce risque et de cette technologie. Je suis à votre disposition pour en discuter.

Cordialement,
Y.





○○○

Hello X,

I am following up on our conversation about Active Directory security.

To quantify the criticality of Active Directory's robustness, you need to understand its central role in the organization: with a few rare exceptions, all our users, applications, hardware, and data depend on Active Directory and its embedded access management system.

From a hacker standpoint, owning our Active Directory is the Holy Grail. It means having access to everything that is vital to us. As a matter of fact, all major attacks in recent years have had a compromised Active Directory at their core. The resulting business impacts span:

- Business continuity - LockerGoga ransomware immobilized Norsk Hydro's entire production, at a cost that will approach €100M. In Denmark, NotPetya caused the Maersk port terminals to close for two days at an estimated cost of \$300M.
- Loss of image and customer trust - The attack on Target cost more than €110M directly and indirectly.
- Direct financial losses - The Carbanak operation has exfiltrated hundreds of millions of dollars from dozens of banks.
- Stock price drop - Yahoo! lost \$350 million in valuation due to their massive breaches, not to mention Uber, whose deal with SoftBank dropped from \$68B to \$48B in one month due to a highly publicized data loss.

But this overexploitation of Active Directory by hackers is also an opportunity for us: by rigorously protecting this critical center, we can defeat an extremely wide range of threats. Alsid is the leader in the field. They have dozens of customers like us who speak highly of their solution. Technically, this technology would have protected us from all the attacks described above. I believe we should launch an assessment of this risk and of this technology as soon as possible. I am at your disposal to discuss it.

Best regards,
Y.





Addressing Active Directory Security

Best Practices

There are several trusted sources which detail the best practices organizations should follow in order to harden and defend their Active Directory. Most notably:

- **Microsoft:** <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>
- **NIST:** <https://nvd.nist.gov/ncp/checklist/669>
- **ANSSI:** <https://www.ssi.gouv.fr/guide/recommandations-de-securite-relatives-a-active-directory>





ALSID for AD

Alsid for AD is an agent-less, cloud-based platform dedicated to Active Directory security.

Alsid hardens your directory infrastructure, enriches your SOC capabilities with AD threat detection, and empowers your incident response and hunting teams into investigating AD-related threats.



ANTICIPATE

Proactively harden your directory infrastructure

Bring vulnerabilities and weak configurations to light and maintain strong security boundaries through time

Threat hunter, Security auditor, Blue team



DETECT

Detect attacks in real time using Alsid's graph-oriented behavioral engine

Make AD security part of your SOC processes through our integrations with SIEM, EDR, SOAR, Orchestrators, etc.

Hunt for stealthy attacks through advanced queries and pattern matching

SOC analyst



RESPOND

Replay attacks and hunt for the patient zero throughout all your AD infrastructures

Remediate with actionable fixes, inform your response plan with levels of priority and criticality, start with quick wins

Incident responder



