ARE YOU COVERED?

Understanding the importance of investing in cyber-insurance

WALLIX
TRACE, AUDIT & TRUST


WALLIX
TRACE, AUDIT & TRUST

'Are you covered?'
Understanding the importance of investing in cyber-insurance

The insurance industry has long been a fixture of business. Lloyds of London, for instance, dates to the 17th century, maintaining a global reputation for meeting the ever-changing requirements for insurance.

In the 17th century the demand was for marine insurance. Today, it's cyber-insurance. In the modern climate, with digitized business processes and data migrating to the Cloud, IT security is the biggest challenge organizations face, with a need to defend against data theft and other cyber-crime in an increasingly digital economy.

It's a sad fact that many businesses, both large and small, will be the subject of a cyber attack. But not all of these attacks are carried out by criminal masterminds. The truth is, data breaches are just as likely to come from someone working within the company who, perhaps unwittingly, has left an opening in the company's defenses that then makes it easier to breach.

Of all reported data breaches in 2017, the majority were the result of insufficient cybersecurity practices, not brute force.

It is no longer a question of if, but when IT data and systems security will be breached – and how bad will it be. It is imperative that robust cybersecurity policies and technologies be in place to prevent cyber attacks and to mitigate the damage when a breach occurs, enabling quick response to minimize losses and keep businesses moving.

Privileged Access Management (PAM) integrates seamlessly with businesses' existing systems for fast and painless deployment and adoption while facilitating robust data security and compliance with strict regulations.

WALLIX
TRACE, AUDIT & TRUST

Data Breaches by the Numbers

As cybercrime increases globally year after year, what exactly are organizations facing in terms of cyberthreats?

- **74% of IT security breaches were achieved through** stolen login credentials
- **74% of data breaches were carried out** by a malicious outsider… meaning that **26% is potentially from an inside source**
- **Only 4% of cybersecurity breaches were "secure" with encrypted data.** An overwhelming 96% of stolen data is unencrypted
- **10.5 million data records are stolen** every day
- And yet, **as of 2017, only 33%** of businesses have a formal cybersecurity policy

The Global Cyber Threat

There is little argument that cyber threats pose a considerable risk to companies worldwide, from Europe to the US, Asia, and beyond. Corporations are by far the biggest victims of cybercrime, with data breaches impacting just about every industry sector. In the U.S. alone, the number of data breaches increased by 29% just in the first half of 2017. **Ponemon** reports that **89% of businesses experience a cyber-attack.**

Who's the most vulnerable (or valuable) for cyber criminals to target?

- **Healthcare**
  25% of all reported data breaches occurred in the healthcare sector, where the security of private data is paramount

- **Finance**
  15% of all cyber-attacks targeted banks, insurance companies, and other players in the financial sector

- **Public Sector**
  23% of reported data breaches were in the Public (10%) and Education (13%) sectors, including government agencies and universities.

The threat of cyber crime is far outpacing organizations' efforts to combat it, leading to a constant stream of media reports recounting the latest devastating breach of personal, financial, or even national security-relevant confidential data.

Costs of Recovering from a Breach

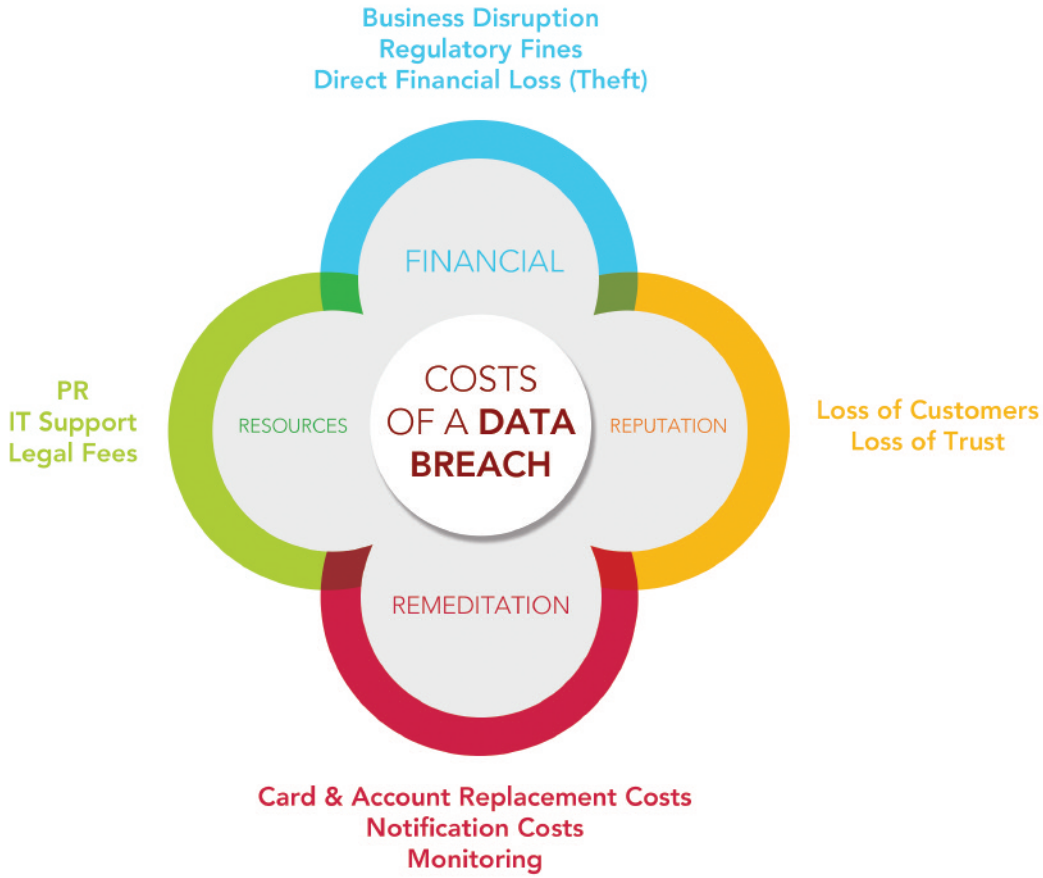
Just as the expectations that a business will experience a cyber incident are increasing, so too are the costs of recovering from those breaches. As of 2018, the global average cost of a data breach is $3.6 million, or about $141 per stolen data record.

Who's suffering the most? Industries subject to strict regulations, like healthcare and energy, experience significantly higher recovery costs. The Healthcare industry reports paying an average $380 per record – more than double the global average. Similarly, the Financial industry reports $336 per stolen record. Science and Industrial sectors trail behind in the mid-200s per record.

Types of Costs Associated with a Cybersecurity Breach

The costs associated with the aftermath of a cybersecurity data breach are varied, and long-lasting. Businesses must pay for everything from hiring specialists to audit the violated systems to notifying the government and individuals that their information was stolen.

Costs of a Data Breach



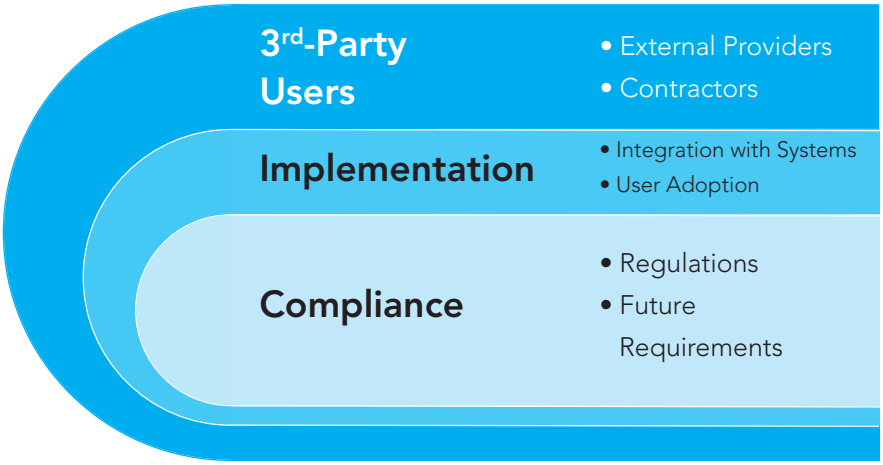
Studies show that it takes, on average, **46 days to resolve** a cyber attack, at an average cost of more than $21,000 per day. And this doesn't even mean the attack has been fully stopped, as some attacks are prolonged or remain dormant and unidentified. In addition, disruption to business-as-usual affects employee process and interrupts productivity, causing losses of up to half of a company's annual income.

In direct costs, businesses can face thousands in fees and fines. There are lawyers to be paid, PR agencies managing the crisis, and exorbitant costs for notifying affected parties and remediating the situation. Not to mention, data breaches can result in hefty fines from regulatory organizations at all levels of government and industry. GDPR, for example, can attract fines of up to 20 million euros – around $23.6 million dollars – for non-compliance.
In terms of reputation, a significant data breach is a breach of trust and confidence in your brand. 76% of consumers would leave a business with a bad cyber track record, leaving breached businesses with reduced revenue for potentially years to come.

For a bit of good news, however, data shows that having an Incident Response team and plan in place dramatically reduces the final costs of a data breach. The Boy Scout's rule to always be prepared truly pays off, literally, when facing a cybersecurity breach.

Modern Security Challenges

In the new, digital age of business, there are a wide variety of factors with implications for cybersecurity, often working in contradictory directions. Organizations face increased, and ever-changing use of external providers needing access to sensitive resources, complex existing systems and processes, and a host of regulatory compliance concerns to contend with.



WALLIX
TRACE, AUDIT & TRUST

Organizations in Flux

Use of external, 3rd-party privileged users is a widespread practice in all industries, but granting access rights to users outside of your organization presents one of the greatest cybersecurity vulnerabilities.

All modern-day organizations, both large and small, rely on highly dynamic and ever-changing workforces, comprising both employees and contractors. And all these staff require access to the organization's IT system.

Companies, then, are faced with the possibility that there are lingering privileged accounts that are long forgotten, or users are holding onto login credentials they no longer need, or users have left the organization but their privileged accounts still exist. Any of these privileged accounts could be used at any time to access private data with malicious intentions.

Proving that access to IT infrastructure is correctly managed is critical, and a lack of visibility around access is a potential risk factor for cyber insurance providers when it comes to deciding to pay out in the event of a breach. Access control, then, is a high-pressure issue for many organizations.

Integration with Systems and Personnel

One of the biggest hurdles organizations face when trying to implement security processes is complications in deployment. As the "digital age" has been upon us for some time now, most businesses have many digitized systems already in place, requiring integration with new security software that can be complex or never quite work properly.

On top of systems, businesses also face pushback in the form of employees themselves. Change management is never easy, and overly complicated security policies are sure to elicit complaints, yet user adoption of good practices – not sharing passwords, granting or revoking privileges only as needed – is crucial to successful cyberthreat defense.

Cyber Standards & Regulations

As the world grows more digital, government and other regulatory bodies have rushed to define minimum standards for data security, industry policies, and cyber practices. Between GDPR, the NIS Directive, PCI-DSS, HIPAA, ISO 27001, SOX, and innumerable other regulations, businesses

might be subject to any number of stringent requirements (and the fines for non-compliance that go along with them).

How's an organization supposed to juggle all these conflicting factors?

Fighting Cyber Crime

In order to combat cybercrime, businesses need an established IT security policy; one that is comprehensive, enforceable, and, perhaps most importantly, easily adopted by users of the systems in question.

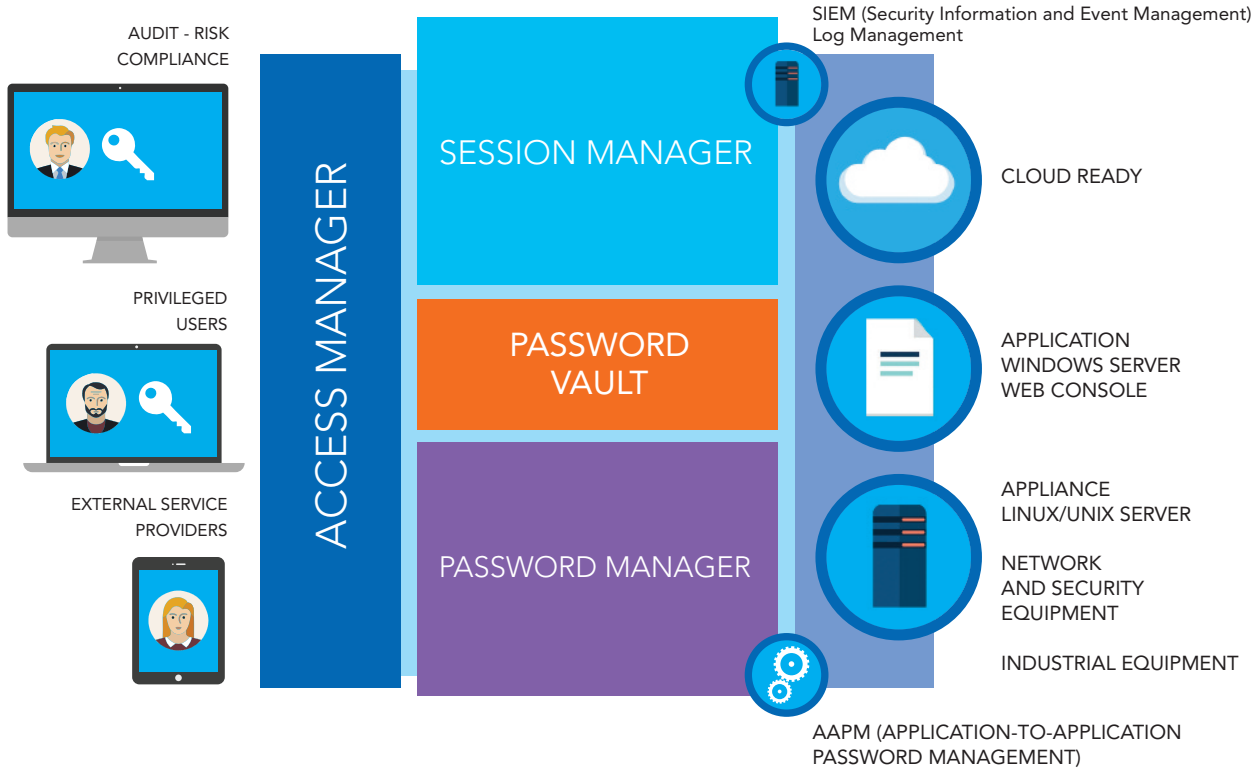
Privileged Access Management is the first line of defense for businesses to protect their most valuable data and systems from breaches. PAM at once prevents security vulnerabilities, reduces cybersecurity risk, and reduces response time (and therefore costs) in the event of an incident through enhanced audit and reporting

Implementing PAM

Regardless of the highly sensitive nature of data or IT resources available to employees, if a password policy or other security measure is not easy to use, if the process is cumbersome or slows down productivity, users will simply avoid it.

A good PAM solution eliminates all of these concerns. The WALLIX Bastion makes PAM – and cybersecurity – simple. With a **Password Manager** to store, rotate, and revoke passwords, and an **Access Manager** to control who can access which resources and when, all privileged activity is funneled through a single access point. And if no user ever needs to know the login credentials to sensitive systems, then there is no risk of them being shared, lost, or stolen.

Beyond usability, a critical aspect of organizational cybersecurity is the need to comply with industry and government regulations and standards. Thankfully, many of these standards have consistent themes between them, requiring for example the application of Least Privilege and control over who has credentials to access sensitive data. Privileged Access Management responds to many regulatory criteria, and thanks to the **Session Manager**, also provides proof of compliance. The WALLIX Session Manager features an unalterable audit log of all privileged session activity for complete oversight, audit, and event response



Controlling Privileged Access

"Privileged Access Management is Cyber Insurance against malicious cyberthreats."

Managing and monitoring privileged access to confidential resources means organizations can rest easy knowing their most valuable data and systems are protected. Privileged Access Management is Cyber Insurance against malicious cyberthreats.

In the current climate of disastrous cyber attacks hitting established organizations once considered bulwarks of their industries, you can't afford not to invest in cybersecurity. Privileged Access Management is your first step to cyber insurance.

WALLIX
TRACE, AUDIT & TRUST

WALLIX

TRACE, AUDIT & TRUST

WALLIX Group is a cybersecurity software vendor dedicated to defending and fostering organizations' success and renown against the cyberthreats they are facing. For over a decade, WALLIX has strived to protect companies, public organizations, as well as service providers' most critical IT and strategic assets against data breaches, making it the European expert in Privileged Access Management.

As digitalization impacts companies' IT security and data integrity worldwide, it poses an even greater challenge if the data involved is highly sensitive. The recent regulatory changes in Europe (NIS/GDPR) and in the United States (NERC CIP/Cyber Security Directorate) urge companies belonging to sensitive sectors to place cybersecurity at the heart of their activity.

In response to these challenges, WALLIX created a bastion designed to secure organizations' core assets while adapting to their daily operational duties: WALLIX Bastion. The WALLIX bastion accompanies more than 100 operators in sensitive sectors to conform with regulations and over 400 organizations in the protection of their critical assets, securing the access to more than 100,000 resources throughout Europe and the MEA region. It was also the first government-certified solution in the market.

WALLIX partners with a trained and certified network of over 90 resellers and distributors that help guarantee effective deployment and user adoption.

WALLIX is the first European cybersecurity software editor to be publicly traded and can be found on EuroNext under the code ALLIX. As one of the leaders of the PAM market, major players trust WALLIX to secure access to their data: Danagas, Dassault Aviation, Gulf Air, Maroc Telecom, McDonald's, and Michelin are among them.

WALLIX is the founding member of Hexatrust. The WALLIX bastion was elected "Best Buy" by SC Magazine and awarded at the 2016 Computing Security Awards, BPI Excellence, and Pôle Systematic.

Twitter: @wallixcom
More information on: www.wallix.com

OFFICES & LOCAL REPRESENTATIONS

WALLIX FRANCE (HQ)
http://www.wallix.com/fr
Email : sales@wallix.com
250 bis, rue du Faubourg Saint-Honoré
75017 Paris - FRANCE
Tél. : +33 (0)1 53 42 12 90
Fax : +33 (0)1 43 87 68 38

WALLIX UK
http://www.wallix.co.uk
Email: ukinfo@wallix.com
1 Farnham Rd, Guildford, Surrey,
GU2 4RG,UK
Office: +44 (0)1483 549 944

WALLIX DEUTSCHLAND
http://www.wallix.de
Email: deinfo@wallix.com
Landsberger Str. 398
81241 München
Phone: +49 89 716771910

WALLIX USA (HQ)
http://www.wallix.com
Email: usinfo@wallix.com
World Financial District, 60 Broad Street
Suite 3502, New York, NY 10004 - USA
Phone: +1 781-569-6634

WALLIX RUSSIA & CIS
http://www.wallix.com/ru
Email: wallix@it-bastion.com
ООО «ИТ БАСТИОН»
107023, Россия, Москва,
ул. Большая Семеновская, 45
Тел.: +7 (495) 225-48-10

WALLIX ASIA PACIFIC
(Bizsecure Asia Pacific Pte Ltd)
Email: contact@bizsecure-apac.com
8 Ubi Road 2, Zervex 07-10
Singapore 408538
Tel: +65-6333 9077 - Fax: +65-6339 8836

WALLIX AFRICA
SYSCAS (Systems Cabling & Security)
Email: sales@wallix.com
Angré 7ème Tranche Cocody
06 BP 2517 Abidjan 06
CÔTE D'IVOIRE
Tél. : (+225) 22 50 81 90

www.wallix.com