Heirs Technologies

The Cost of Trust

A Guide to Cybersecurity & Digital Trust in the AI Era

TABLE OF CONTENTS

Introduction:
The Trust Imperative

Organisations no longer compete on products and price alone. Trust is quickly becoming the ultimate differentiator, and digital trust has an unforgiving fracture point, cybersecurity.

A single cyber incident can vaporise decades of brand equity overnight. Businesses are now learning this lesson from incidences and newspaper headlines, and not just from white papers and case studies anymore. In September 2023, MGM Resorts watched its Las Vegas empire grind to a halt. Slot machines went dark, room keys stopped working, guests were locked out, all because a ransomware gang exploited a single layer of identity. The estimated cost was over $100 million in lost revenue and remediation, not to mention an international reputational bruise that will take years to heal.

Rewind to May 2021. Colonial Pipeline, the artery carrying nearly half the United States' east coast fuel supply, fell victim to a password leaked on the dark web. The CEO authorised a $4.4 million ransom payment as panic-buying emptied petrol stations while the White House scrambled. Beyond the operational paralysis, the breach exposed the uncomfortable truth that critical infrastructure trust can be shattered by an unpatched VPN or a single compromised credential.

consider the data:

$4.45M

Average Cost of One Data Breach

$4.45T

Annual Global Cost of Cybercrime

> *If Cybercrime were a country, it would rank as the world's third largest economy.*

According to PwC's research, 87% of consumers will take their business elsewhere if they don't trust a company to handle their data responsibly.

So, what makes trust so fragile? Digital transformation has dissolved the traditional perimeter. Cloud adoption, remote work, IoT, AI-driven supply chains and third-party ecosystems have created an interdependent web where a weakness in one node can cascade into a systemic crisis. Attackers no longer just steal data; they extort, they embarrass, they erode the implicit promise a brand makes: "You are safe with us."
Yet many organisations still treat cybersecurity as a compliance checkbox. Compliance is not trust. Compliance proves you followed a baseline; trust proves you value what you protect.

The question isn't whether your organisation will be tested. The question is whether, when that moment comes, your partners, your clients and your stakeholders will say, "We trust them to get this right."

In the digital economy, trust is no longer a by-product of success. It is the prerequisite for it.

Every Business is Now a **Technology Business**

Imagine walking into a bank. You see polished marble, tellers behind glass, a vault door thick as a promise. But the real bank isn't there. It's an invisible constellation of cloud instances, real-time APIs, and millions of lines of code processing billions of transactions before you blink. The bank itself is a technology company that happens to hold a banking licence. This is the inevitable destination of every industry on earth, and it completely redefines what must be protected.

Banks as Technology Companies

JPMorgan Chase employs over 55,000 technologists and spends roughly $15 billion a year on technology. That's more than the entire revenue of many Silicon Valley giants. Why? Because a modern bank is a software platform delivering financial services at scale. From mobile cheque deposits to real-time cross-border payments, the product is code.

When this digital reality is interrupted, the consequences are instant. In 2019, a misconfigured web application firewall at Capital One exposed the personal data of over 100 million customers. A single config error turned into a $190 million class-action settlement and an immeasurable erosion of trust. Banks solvency now depends on code integrity as much as on capital reserves.

Manufacturers as Technology Companies

The factory floor is no longer a world of purely physical labour. It is a web of industrial control systems, IoT sensors, and AI-driven supply chain orchestration. A modern automotive plant can produce a vehicle every sixty seconds, but that cadence stops the moment a digital link breaks.

A script played out in 2021 when JBS Foods, the world's largest meat processor, suffered a ransomware attack that halted operations across the US and Australia. The disruption sent tremors through the food supply chain, proving that even beef, pork, poultry are now digital goods until the moment they land on a plate.

JBS FOODS
2021

Ransomware Attack

- Production halted
- US & Australia affected
- Food supply disrupted

Why governments are increasingly attacked

If banks are digital and hospitals are digital, then the machinery of the state is the ultimate digital prize.

Governments manage

- elections
- social services
- defence logistics
- tax collection
- and public health

all through interconnected technology stacks. The threat is no longer confined to espionage. Digital paralysis can destabilise entire nations, making a pillar of national sovereignty.

The story is the same whether the product is money, cars, surgery, or public trust: the business is the technology. Every transaction, every patient record, every assembly line robot, every citizen service portal is a node on a vast digital nervous system.

Whether you manufacture products, move goods, or provide services, your business now runs on technology, and technology risk is business risk

The
Threat Landscape

The same broadband that enables mobile payments, remote power-grid management, and cross-border e-commerce also delivers ransomware, business email compromise, and state-sponsored espionage. Nigeria alone lost an estimated $500 million to cybercrime in 2022. Let's look at what has already happened globally and how it unfolded.

~$500M

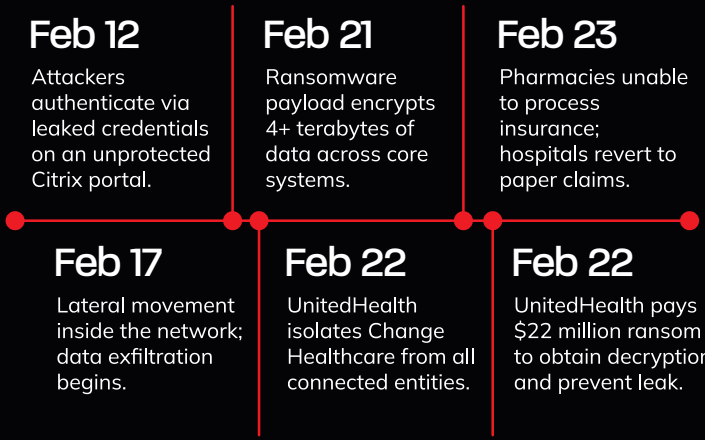
lost to cybercrime in Nigeria in the year 2022.

Ransomware

Attackers encrypt critical systems and data, then demand payment. Modern gangs steal sensitive files first and threaten to publish them, turning a disruption into a brand-destroying data leak.

Real Incident: Change Healthcare (February 2024)

Change Healthcare, a subsidiary of UnitedHealth Group, processes 15 billion healthcare transactions annually and roughly one in three US patient records. On February 12, attackers from the ALPHV/BlackCat ransomware gang gained entry through a Citrix remote-access portal that lacked multi-factor authentication. The compromised credentials, likely purchased from a dark web broker, gave them a foothold.

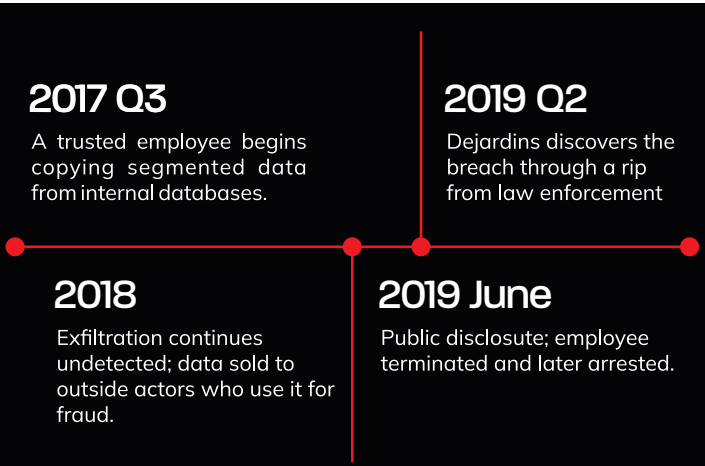


Insider Threats

Not all danger arrives from an external IP address. Insiders such as disgruntled employees, careless staff, or malicious hires, can weaponise legitimate access to exfiltrate data, sabotage systems, or sell secrets. They already have the keys and often know precisely where the jewels are stored.

Real Incident: Desjardins Group (2017–2019)

Desjardins, the largest credit union federation in North America, suffered one of the largest privacy breaches in Canadian history. A marketing department employee methodically copied sensitive personal and financial data of 9.7 million individuals and sold it to third-party fraudsters over a 26-month period.



Impact

- $200.9 million class-action settlement, one of Canada's largest privacy payouts.

Behavioural analytics can catch anomalies. This employee moved data in patterns that should have triggered automated alerts if properly monitored. Why did one marketing employee have bulk access to 9.7 million records?

Supply Chain Attacks

Attackers compromise a trusted software or service provider, then use that trusted channel to push malware downstream to the provider's client base. The victim opens the door because the update or integration arrives bearing a familiar, signed certificate.

Real Incident: Kaseya VSA (July 2021)

Kaseya VSA, a remote monitoring and management platform used by thousands of managed service providers (MSPs), was exploited via a zero-day vulnerability. The REvil ransomware group pushed a malicious update that paralysed approximately 1,500 downstream businesses, including the Swedish grocery chain Coop, which had to close 800 stores for nearly a week.

July 2

REvil exploits a previously unknown vulnerability in Kaseya's on-premises VSA server.

Malicious update distributed to all managed endpoints of the affected MSPs.

July 3

Coop Sweden shuts stores after point-of-sale systems became inoperable.

July 4

Kaseya receives a universal decryptor from a trusted third party; recovery begins.

AI-Powered Phishing

Generative AI enables attackers to craft hyper-personalised, grammatically perfect phishing emails, voice notes, and even video messages that bypass traditional spam filters and human scepticism. The old advice to "look for spelling mistakes" is obsolete when large language models can write in a CEO's exact cadence.

Real Incident: Desjardins Group (2017–2019)
A finance employee in the Hong Kong office of global engineering firm Arup received an email, supposedly from the UK-based CFO, requesting a confidential urgent transaction. The employee was then invited to a multi-person video conference where every participant, including the face and voice of the CFO, was an AI-generated deepfake. Convinced, the employee authorised HK$200 million (US$25.6 million) in transfers.

Jan 2024

Attacker uses AI to study publicly available speeches and internal communications of executives

Feb 2

Employee receives an AI-crafted phishing email referencing real internal projects.

Feb 3

Employee attends a multi-party deepfake video call with lifelike recreations of colleagues.

Feb 3

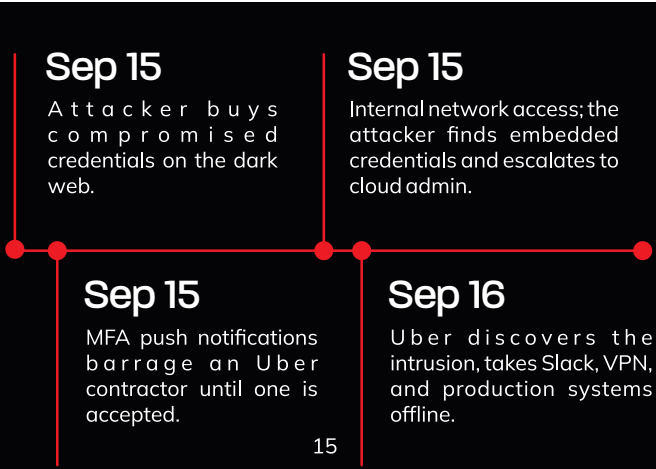
Transfers initiated; funds move through a chain of accounts before disappearing.

Credential Theft

Attackers obtain usernames and passwords via brute-force, phishing, dark web purchases, or keyloggers. With valid credentials, they bypass most perimeter controls and appear as legitimate users. This is the "break-in that looks like a login."

Real Incident: Uber (September 2022)

An 18-year-old hacker associated with the Lapsus$ group purchased stolen Uber credentials from the dark web. When multi-factor authentication (MFA) blocked the login, the attacker launched an MFA fatigue attack, repeatedly sending push notifications to the victim's phone until, out of frustration or confusion, they approved one. Once inside, the attacker discovered PowerShell scripts containing hardcoded admin credentials, granting near-total access to Uber's cloud infrastructure on AWS and Google Cloud.

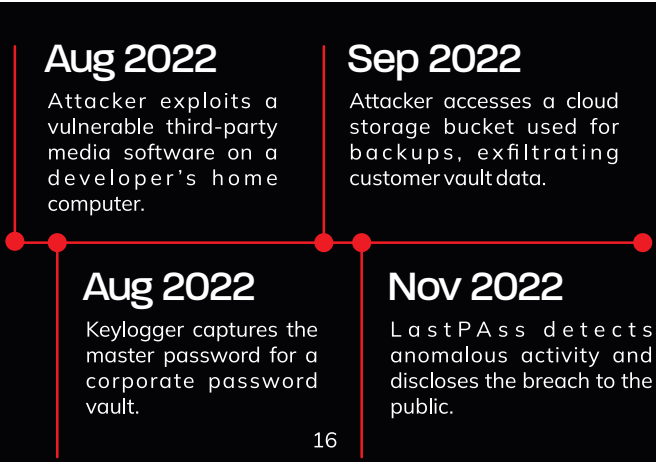


Cloud Attacks

Misconfigurations, exposed storage buckets, insecure APIs, and compromised cloud identities allow attackers to infiltrate or exfiltrate at massive scale. The shared responsibility model means that even if the cloud provider is secure, your configuration may not be.

Real Incident: Uber (September 2022)

A threat actor compromised a software vulnerability on a senior DevOps engineer's home computer, installing a keylogger. This captured the engineer's master password, which unlocked a cloud-based storage environment containing decryption keys for customer vault backups. The attacker subsequently exfiltrated fully encrypted vault data along with metadata URLs a treasure trove for targeted spear-phishing and brute-force attempts.

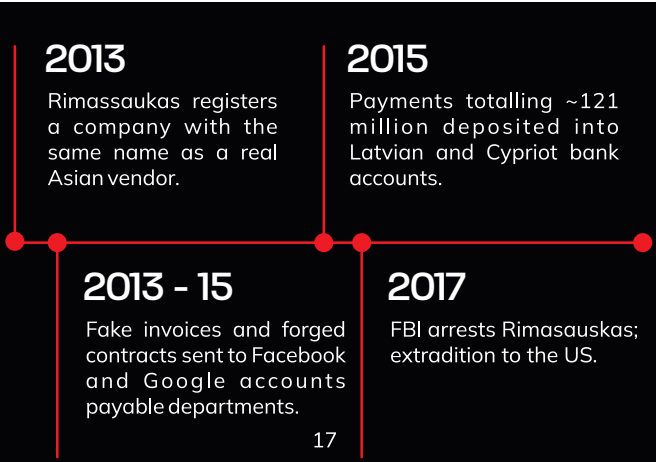


Business Email Compromise (BEC)

BEC attacks involve spoofed or compromised email accounts that trick employees into wiring funds or sharing sensitive data. These attacks are low-tech, high-return, and exploit human psychology rather than software vulnerabilities, but their financial devastation can exceed ransomware.

Real incident: Facebook & Google (2013–2015)

Evaldas Rimasauskas, a Lithuanian fraudster, set up a fake company mimicking the identity of a legitimate Taiwanese hardware vendor that both tech giants used. Over two years, he sent meticulously crafted invoices and contracts, impersonating vendor executives, and convinced both Meta and Google to wire over $121 million in aggregate. The scheme was only discovered when the real vendor asked about overdue payments.



Nation-State Attacks

State-sponsored groups operate with immense resources, patience, and strategic intent. Their goals range from espionage to infrastructure destruction. Unlike cybercriminals who seek quick profit, these adversaries play the long game and often lie dormant inside networks for months or years.

Real Incident: Viasat KA-SAT (February 2022)

Hours before Russia's invasion of Ukraine, the GRU-linked Sandworm group deployed the "AcidRain" wiper malware through a misconfigured VPN appliance on Viasat's KA-SAT satellite network. The malware bricked thousands of modems across Ukraine and Europe, severing military communications and simultaneously knocking offline the remote monitoring of 5,800 wind turbines in Germany.

Feb 23

Attackers compromise a misconfigured VPN in the KA-SAT ground segment

Feb 23

Malicious command pushes AcidRain wiper to tens of thousands of modems at the pre-drawn hour.

Feb 24

Modems rendered permanently inoerable; broadband goes dark across Ukraine and parts of Europe.

Feb 24

Post-incident: German wind turbines lose remote connectivity, requiring manual intervention to maintain grid stability.

The Human Factor

People remain the biggest vulnerability.

You can harden servers, encrypt data, and deploy next-generation firewalls. Yet the most sophisticated defence in the world can be undone by a single human moment: a well-intentioned click, a tired reuse of a favourite password, a finance officer who genuinely believes she's speaking to the CEO.

The human brain is the one operating system that can't be patched with a software update. It craves trust, suffers from cognitive overload, and can be manipulated with alarming precision. Understanding the human factor is more about designing an organisation where human nature is anticipated, and less about apportioning blame.

There are five dimensions of human vulnerability. Each is ancient in its psychological roots but devastatingly modern in its financial consequences.

SOCIAL ENGINEERING

This is the art of manipulating people into revealing confidential information or granting access. It preys on fundamental human traits like helpfulness, fear, curiosity, and respect for authority. The attacker rarely uses a zero-day exploit. They simply pick up the phone or craft a convincing message.

PASSWORD FATIGUE

The average employee juggles dozens, sometimes hundreds, of accounts. Faced with frequent password changes, complexity rules, and the sheer volume of logins, the human brain takes a shortcut: reuse. A password created for a decades-old online forum becomes the key to the corporate VPN. This password fatigue creates a chain of vulnerability where a breach at one site unlocks many more.

INSIDER RISKS

Insider risks range from the malicious, disgruntled staff stealing data for revenge or profit, to the careless, well-meaning employee who accidentally exposes a database.

EXECUTIVE FRAUD

Often called CEO fraud, it is a targeted form of Business Email Compromise where the attacker impersonates a senior leader (CEO, CFO, or board member) to authorise urgent, high-value transfers. The psychology is brutally effective; hierarchy, time pressure, and the illusion of authority combine to short-circuit a subordinate's normal verification habits.

BUSINESS EMAIL COMPROMISE

BEC is the broader category of fraud in which attackers use compromised or spoofed email accounts to manipulate employees into making unauthorised payments or disclosing data. While CEO fraud impersonates internal leaders, BEC also includes vendor impersonation, fake invoice schemes, and account takeover.

The human factor is a constant that needs to be designed for. Every social engineering phone call, every reused password, every obedient wire transfer follows a predictable psychological script. Organisations that understand this train their people and also build systems that make the right behaviour the easy behaviour, and the wrong behaviour nearly impossible.

Technology can reduce risk, but people determine resilience

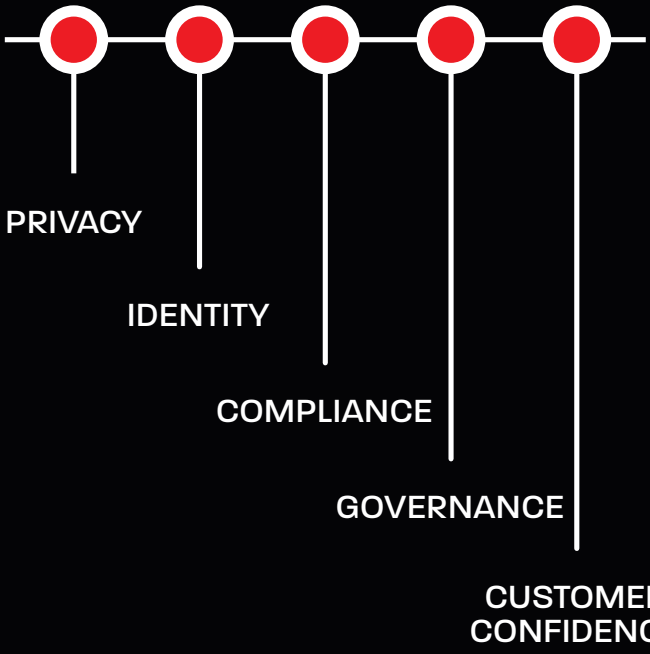
Digital Trust

Cybersecurity stops the breach. Digital trust rebuilds the world the breach tried to shatter.

It's tempting to believe that if your firewalls are hardened, your endpoints patched, and your SOC humming, you've done your job.

A business that is merely secure is a locked safe in a dark room. A business that inspires digital trust is a fortress with the lights on and the doors open. It is inviting, reliable, and visibly accountable. Trust is a hard, measurable, competitive asset in an age where a data scandal can erase a billion dollars of market capitalisation overnight.

The Five Pillars of Trust



i. PRIVACY

The Cambridge Analytica scandal of 2018 remains the defining cautionary tale. Facebook had not been hacked in the traditional sense; its own data-sharing ecosystem had allowed a personality quiz app to vacuum up the personal information of **87 million users,** which was subsequently used for political micro-targeting without consent. The scandal erased **$119 billion** from Facebook's market value, because users realised the platform's relationship with their privacy was transactional, not protective.

Fines are the floor. The real cost of privacy failure is abandonment. The great idea is to turn a regulatory burden into a brand differentiator, thereby command premium loyalty.

> *"The true cost of a privacy breach isn't the fine, it's the loss of trust.*

ii. IDENTITY

Every digital interaction begins with the question “Who are you, and can you prove it?” Identity is the cornerstone of digital trust because it governs the first act of access. A system that cannot reliably verify identity is a system that will inevitably be breached.

Modern identity architectures go beyond passwords and Personally Identifiable Information (PII). Biometrics, behavioural analysis, passwordless FIDO2 standards, and decentralised identity models have set a new pace in the landscape. Microsoft, for example, now blocks 1,000 password attacks per second by moving to passwordless authentication.

Identity also cuts the other way. Customers want seamless access without endless friction. Digital trust is earned when an organisation verifies you with such precision and grace that you never notice e.g. when your face unlocks your bank app and the transaction completes before you’ve exhaled.

1,000

Password Attacks Blocked Every Second by Microsoft

iii. COMPLIANCE

Compliance is the codified minimum. It is society's way of saying, "This is the bare floor beneath which you cannot fall." And yet, many organisations mistake compliance for trust, as if checking a regulatory box will satisfy a customer who just watched their data appear on the dark web.

In 2018, Marriott disclosed that its Starwood guest reservation database had been breached, exposing the records of up to 500 million guests. Marriott had been PCI DSS compliant. It had passed audits. It had the certificates. But the intruders had been inside the network, undetected, since 2014.

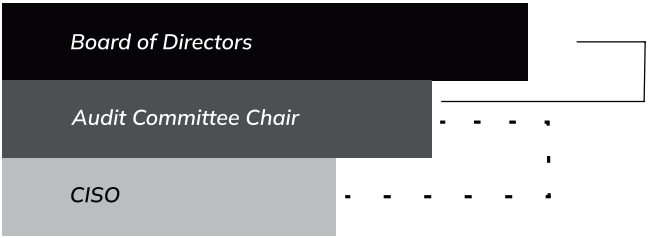
> *"Forward-thinking organisations now treat regulations like GDPR, CCPA, and emerging AI governance frameworks as springboards, not straitjackets.*

They embed privacy-by-design and security-by-design into their product development lifecycle. They voluntarily publish transparency reports. They pursue certifications like ISO 27001 and SOC 2 Type II not because a customer demands them, but because they want to be evaluated. They understand that in the trust economy, audits are not an ordeal to survive but a stage on which to perform.

iv. GOVERNANCE

If compliance is the floor, governance is the blueprint. It answers the question: Who is accountable for trust, and what decision rights do they hold? Without governance, cybersecurity budgets get allocated to the loudest department, incidents are hidden for fear of careers, and the board receives a quarterly traffic-light chart that conveys nothing.

Effective governance means the CISO has a dotted line to the audit committee chair. It means cyber risk is quantified in the language of the business; dollars, market share, reputation, not technical severity scores. It means that when an incident occurs, the organisation has already rehearsed its response, and the decision about whether to pay a ransom or notify regulators is made with the same rigour as a capital allocation decision. Trust is built on the knowledge that the organisation is governed by principle.



v. CUSTOMER CONFIDENCE

Customer confidence is where privacy, identity, compliance, and governance converge and become visible. It's the moment a user clicks "buy" without hesitation, shares their health data without dread, or stays loyal after a breach because the organisation's response was swift, transparent, and humane.

A Deloitte study found that trust-driven companies outperform their peers in revenue growth by up to 3.5 times. And when trust breaks, the punishment is swift: 1 in 3 consumers will abandon a trusted brand after a single bad experience, and data misuse is the ultimate bad experience.

Consider the contrasting fates of two companies after major incidents. In 2013, Target suffered a massive breach affecting 41 million payment cards. The initial response was slow, the communication defensive, and the CEO resigned. It took years for Target to recover both financially and reputationally. In 2017, when the NotPetya malware crushed Maersk, the company mounted an extraordinary recovery, communicating transparently with customers and the public, even as it rebuilt 4,000 servers and 45,000 endpoints in ten days. Maersk's candour and operational heroism preserved customer relationships and the brand emerged with its integrity intact.

Why trust outperforms technology alone

Organisations that merely deploy technology treat security as a product they've purchased. Organisations that inspire trust treat security as a promise they keep. The difference shows up in customer retention rates, in the speed of regulatory approvals, in the valuation premium that acquirers assign to a trusted brand.

A secure company can still be a distrusted one. A trusted company is always, by necessity, a secure one. The goal is not to choose between security and trust, but to recognise that security is the foundation on which the temple of trust is built. Without the foundation, the temple collapses. But without the temple, the foundation is just concrete in the ground.

Digital trust is earned through every secure interaction, every protected identity, and every fulfilled promise.

The Boardroom Questions

Cybersecurity now takes place in the boardroom, alongside discussions of quarterly earnings, market expansion, and executive compensation. The days of the board nodding through a single PowerPoint slide titled “IT Security Update” are over.

But most boards suffer from a lack of a shared language. Cybersecurity is dense with acronyms, technical metrics, and fear-based reporting that makes it difficult to separate signal from noise. The following questions are designed to bridge that gap and to equip directors, CEOs, and C-suite leaders with the precise, business-contextualised inquiries that turn cyber risk from a terrifying unknown into a governed, measurable function.

> *Cybersecurity is no longer an IT conversation, it is a leadership responsibility.*

A Practical Executive Checklist

Use the following questions as a standing agenda for every cyber risk review. If the answer to any question is “we don’t know” or “we’ll get back to you,” the board has just uncovered a risk that requires immediate attention.

- What are our critical assets, and do we have a ranked, tested recovery plan for each?
- How quickly can we detect a serious intrusion, and is that number improving?
- Which third-party relationships pose the greatest cyber risk, and how are we governing them?
- Who is the named executive accountable for cyber risk, and how does the board exercise oversight?
- Where does our sensitive data reside, and is the inventory current?
- Can we recover within our defined Recovery Time Objectives (RTOs), and have we proven it through a live exercise?
- Are we measuring resilience outcomes, not just compliance inputs?

These questions do not require a technical degree to ask, and they do not accept technical jargon as an answer. They demand the same clarity, rigour, and evidence that the board applies to financial audits, legal compliance, and strategic investments.

From Strategy To Execution

The trust economy. The vanishing perimeter. The anatomy of an attack. The human factor. The board's obligation to ask better questions. But a map, however detailed, doesn't move you across the landscape. Only execution does.

Most organisations don't suffer from a shortage of cybersecurity awareness. They suffer from a gap between the strategy they have articulated and the reality they can deliver. They know they need Zero Trust. They know they need resilience, not just compliance. They know the board should see a risk dashboard, not a patch-count. But knowing and doing are separated by a chasm of complexity, legacy systems, talent scarcity, and competing priorities.

Strategy defines the destination. Execution covers the ground. Heirs Technologies exists to ensure that the distance between them is as short, as certain, and as secure as possible. We translate the imperatives explored in this booklet into operational capabilities that scale, adapt, and endure.

Welcome to execution. Let's begin.

Visit our website ***www.heirstechnologies.com*** *to book a free consultation.*

www.heirstechnologies.com
support@heirstechnologies.com | +234-201-888-9719
| @ heirstechnologies