5 Major Financial Risks
CFOs Don't Hear About from IT

The events of 2023 reveal that C-level executives continue to underestimate the severe adverse impact cyberattacks can have on the long-term health —and even the survival—of their business.

Here's what you need to know to make smarter risk/reward decisions in 2024.

Executive summary

Cyberattacks continue to take their toll on companies large and small. Yet, despite their theoretical role as primary guardians of their organizations' exposure to financial risk, CFOs remain largely disengaged from the challenge of cyberdefense.

This CFO disengagement is due to the fact that cybersecurity has historically been viewed as a purely technical discipline for which the IT department is exclusively responsible.

Technology, however, is now a pervasive element of every business. So CFOs must assume appropriate leadership of their organizations' efforts to minimize their exposure to technology-related risk.

More specifically, CFOs and other C-level executives must fully recognize that today's ever-intensifying expose their organizations to financial risks that go well beyond the short-term impact of downtime.

Only by fully understanding these risks can CFOs effectively address them. And without such an understanding, CFOs will leave their organizations unacceptably exposed to such risks —potentially threatening their financial performance, as well as their very survival, in 2024.

In addition to downtime, **these five other major risks** associated with cyberattacks can devastate a company's top- and bottom-line financial performance in both the short term and the long term:

- **Loss of future revenue**
- **Loss of company value**
- **Uninsurability**
- **Legal and regulatory exposure**
- **Supply-chain disruption**

vCSO Magazine

The 2024 cyberthreat landscape

As 2023 draws to a close, one unfortunate reality remains clear: Businesses large and small are suffering significant financial harm from cyberattacks. From the massive takedown of MGM Resorts to the 14,000 smaller companies that had their WordPress websites hijacked, cyber attackers are wreaking havoc on their victims using tactics and techniques that constantly evolve in response to the cyber defense methods business employ in the hopes of thwarting them.

And those attacks are intensifying in volume. Overall, the estimated increase in attack intensity rose about 7% from 2022 to 2023, with a similar increase projected for 2024.

But the real concern for business leaders isn't attack intensity per se. It's the actual financial damage those attacks could inflict. And that financial damage is projected to grow by more than 17% globally next year—from approximately $8.5 trillion in 2023 to $10 trillion in 2024.

Several factors account for this continued escalation in cyberattack intensity, including:

Cybercrime pays. Once upon a time, hackers hacked for sport. No longer. Cybercrime is now a for-profit activity that often pays off for its practitioners. And it pays off in cryptocurrency, which now provides the ideal untraceable means of payment—whether from victim to attacker or attacker to a third-party data "fence" on the Dark Web.

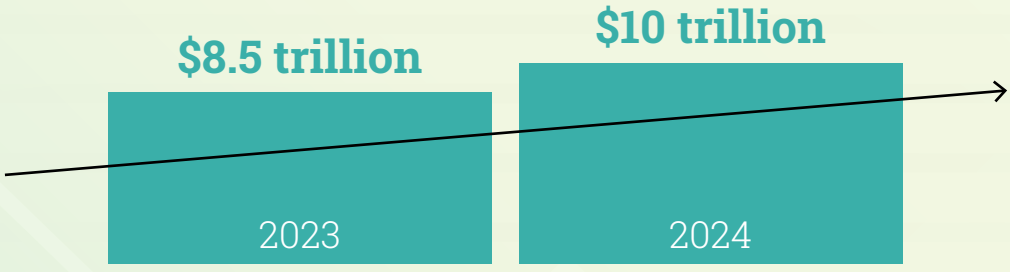
Ransomware attacks have proven especially lucrative, as businesses will often pay attackers to rescue business-essential data that has been rendered inaccessible by encryption. Alternatively, knowing the concerns executives have about the negative publicity that an attack can generate, attackers these days often simply blackmail companies by threatening to publicly reveal the success of their attack unless they receive a large payment.

Attackers can also profit by selling the personally identifiable information (PII) they steal form a company's customer database on the Dark Web—or by selling proprietary business information to competitors as "business intelligence."

Cybercrime-as-a-service. There was also once a time when cyber criminality required exceptional cyber skills. Hackers not only had to be expert coders. They also had to spend countless hours studying cyber defenses in order to uncover the hidden needle-in-a-haystack weakness in those cyber defenses. They then had to engineer a clever method for exploiting those weaknesses—and then devote even more time to searching out targets that might be vulnerable to the clever method they had just personally engineered.

This twin barrier of skill and time is gone. The Dark Web is now an open marketplace for cybercrime tools and targets. So instead of developing an attack method themselves—and then seeking out targets whose technology profiles best align with that method—wanna-be cybercriminals can simply shop for both, just like a legitimate business would shop for legitimate business software and a legitimate business marketing list.

Financial impact of cybercrime



Financial damage is projected to grow by more than 17% globally next year—from approximately $8.5 trillion in 2023 to $10 trillion in 2024.

In some cases, criminals can even order fully turnkey cyberattacks the same way you'd order a ride from Uber or a meal from DoorDash. Becoming a cybercriminal thus requires little more than a stash of cryptocurrency and the desire for ill-gotten gains.

Increased activity of state actors. As global geopolitical tensions escalate, so has the activity of state actors seeking to disrupt their perceived adversaries via cyberattacks. Chief among these state actors are China, Iran, North Korea, and Russia—which have spent years developing sophisticated and highly scalable cyberwarfare capabilities. As cyberwarfare evolves to become an intrinsic component of all military strategy, however, many other countries are developing their own cyberwarfare units.

Historically, state-actors attacks have mainly targeted government systems such as Department of Defense, elections, and public-sector finance. But cyberwarfare tactics have shifted noticeably in recent years to include the private sector as well. Infrastructure-related enterprises are now key targets as well. Energy utilities, for example, have seen
a precipitous 40% increase in attack intensity

And no business is exempt from cyberattacks by state actors—because once such an attack is launched, it can propagate indiscriminately to any vulnerable organization. The WannaCry attack launched by North Korea, for example, infected 200,000 computers across 150 countries with ransomware before it was eventually neutralized.

60%

of breached organizations had to **raise prices** to customers due to the cost of the breach

The AI arms race. Artificial intelligence (AI), machine learning (ML), Natural Language Processing (NLP), neural networks, and other self-enhancing technologies are dramatically changing the face of software. And many of those changes are benefiting businesses with better, more efficient ways of getting things done.

Cybercriminals are, of course, also taking advantage of advances in AI to better penetrate cyber defenses. For example, they're using AI to create "deep fake" images, videos, and voices that more readily deceive employees. They're also using AI to automate the creation of new kinds of malware that can modify themselves just enough to fool their targets' cyber defenses—while still maintaining the functional ability to achieve their desired nefarious ends.

More tech in more places. Businesses of all kinds continue to deploy more technology, subscribe to more cloud services, and generate more data. As their digital footprints grow in these ways and others, so do their "threat surfaces"—i.e., the number of potential points-of-infiltration for a would-be attacker.

Other trends further increase the vulnerability of businesses to cyber criminality. The big upsurge in employees working from home, for example, puts an added strain on a company's defenses against illicit remote access. Cyber defenses are also being strained as businesses outsource functions that were formerly performed by in-house staff—requiring them to provide systems access to a growing and ever-changing cast of suppliers, subcontractors, and strategic partners.

Bottom line: More technology inherently exposes businesses to greater technology-related financial risk.

The role of the CFO

Primary responsibility for managing financial risk falls squarely on the shoulders of the CFO. That's because CFOs are uniquely qualified to:

- **Identify, analyze, and quantify** risks to financial performance
- Determine which risks should be **reduced** with safety measures (and how to right size/ prioritize resource allocation accordingly)
- Determine which risks should be **transferred** to an insurer (and what coverages, conditions, and premium costs are appropriate for those risks)
- Determine which risks should be **avoided** by simply not doing that which causes the risk
- Determine which risks should simply be **accepted**
- Advise CEOs and boards about the **current risk state**
- Advise CEOs and boards about the risks associated with any **decisions currently under consideration**, so that those decisions can be made with their risk factors and risk management costs "baked in"
- Continuously **track risk over time** to respond to changes in the magnitude, nature, and manageability of risks—as well as to drive continuous improvement in risk management tactics and processes.

Unfortunately, CFOs tend to do very little of this when it comes to cyber risk, despite the growing magnitude of that risk.

In fact, according to the Deloitte Center for Controllership, in only about 20% of organizations do CFOs work closely with IT to understand and take a central role in the management of cyber risk.

This lack of involvement is especially remarkable given that 34.5% of these exact same organizations have experienced at least one attack on their financial data.

Several factors may contribute to CFOs' lack of involvement in their organizations' cyber risk challenges. One factor is that cyber risk is often viewed as a purely technical issue. So CFOs believe that their own lack of technical knowledge renders them insufficiently qualified to understand and participate in the mitigation of risks associated with their organizations' ever-expanding digital environment.

Another factor may be that CFOs and their functional equivalents already have their hands full with other sources of risk. Rapidly rising interest rates, concerns about climate change, the COVID pandemic, chip shortages, and other financially impactful developments have made the past few years quite challenging for CFOs. So it's only natural that they would defer deeper engagement with technology-related risks that, at least theoretically, are already under the aegis of IT.

But this non-engagement is no longer tenable for three reasons:

1. **The magnitude of cyberrisk is too great to escape the essential involvement of the CFO.** Cyberattacks represent an existential threat to every company. CFOs need to acknowledge that fact and engage accordingly.
2. **IT is not equipped to address risk from a true financial/business perspective.** Technologists approach issues such as hacking and insider threats as technical issues with technical solutions. They are neither positioned not qualified to assess the potential adverse financial impact of cyberrisks on the business, formulate the most financially prudent approaches to managing cyberrisk as a whole, or ensuring that the management of cyberrisk is well-integrated and aligned with the organization broader risk management strategy.
3. **Technology-related risk is intimately connected to all other financial risk.** If you're mitigating supply-chain risk by increasing your inventories, you're using technology to maintain those new inventory targets. If you're mitigating your exposure to the risk of business fraud with appropriate process controls, you're using technology to implement and enforce those controls. Technology touches every aspect of financial risk—and every aspect of the business is touched by technology risk.

CFOs work with IT to manage risk in only **20%** of organizations.

5 Major Financial Risks CFOs Don't Hear About from IT

Everyone knows hackers out there. And everyone knows getting hacked is bad. But CFOs can't fulfill their critical role as risk management leaders with nothing but a vague, generalized sense that cyberattacks can inflict financial harm. They need a clear sense of what those financial harms could be—both in terms of nature and magnitude.

One of those financial harms is downtime. If a cyberattack paralyzes an organization's IT systems, that organization is for all intense and purposes incapacitated. And that incapacitation can last for hours, days, or even weeks.

Downtime means that a company can no longer serve its customers. So it will lose customers and/or need to issue costly refunds. It also means people won't be able to perform productive work. So there's no sales, no production, no marketing, no customer support, no logistics, no hiring, no purchasing, and of course no accounting.

The immediate cost of downtime is obviously significant. And it can be readily calculated based on numbers readily available to most CFOs: weekly sales performance, active order pipeline, revenue per employee, etc.

Downtime is also the impact that IT is most likely to discuss—since systems uptime is a core IT KPI. So downtime is a direct threat to IT's performance mission.

But the immediate operational impacts of downtime are not the only financial risks associated with cyberattacks. In fact, those immediate impacts are often not even the biggest risk to businesses from a long-term financial perspective.

CFOs and their executive peers should therefore understand, assess, and address the following five financial risks that their IT departments typically do **not** include in their cybersecurity conversations.

Those 5 impacts are:

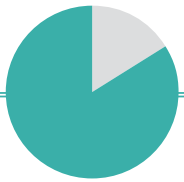
Financial Impact 1

Loss of future revenue

Downtime doesn't just impact sales during the downtime event itself. Downtime can also have a significant adverse impact on sales performance in the future. And that impact can remain persistent years into the future.

That's because many of the customers who are alienated during the downtime event will take their business elsewhere and never come back. And because those customers don't come back, they can't be a source of referrals for other new customers or generate word-of-mouth marketing—which, depending on factors such as vertical market and sales channel can drive 22-46% of prospects into an organization's sales pipeline and ultimately be a primary contributing fact to as much as 84% of all net-vnew sales.

Failure to reach that initial set of new customers, in turn, means loss of another set of potential referrals and word-of-mouth brand advocates. **The knock-on effect of these successive lost opportunities for future sales is thus typically a multiple of a company's current revenue**—which means that as a financial risk it can be of significantly greater magnitude than any immediate loss of sales.



A cyberattack can cost a company up to **84%** of all **future net-new sales**.

Financial Impact 2

Loss of company value

Cyberattacks don't just alienate customers. They also alienate investors, as well as the executive leadership of any other company considering a merger or acquisition of the affected entity. Just ask anyone who's seen a pending M&A deal fall through due to an untimely cybersecurity incident.

That's because **cyberattacks are seen by these financially minded individuals as possible indicators of some kind of broader management deficit**—whether that deficit is one of competence, culture, or attention to detail. A major attack thus raises a question in their minds: "Are the problems in this organization that made it vulnerable to hacking symptomatic of an underlying issue that make it a bad risk more generally?"

The case of MGM Grand, which was hit by a major cyberattack in September 2023, offers a prime example of this valuation loss. The company reported about $80 million in immediate losses due to the downtime incurred due to the attack. But the real damage was the half-billion drop in its stock price.

Even for smaller companies that are not publicly traded, the same math still applies. A cyberattack can have the same impact on a company's valuation as a product recall, a lost lawsuit, or any other incident that calls the credibility of its management and/or its operating standards into question.

2023 cyberattack resulted in:

$80 million in downtime losses

$500 million in lost valuation

Financial Impact 3

Uninsurability

As noted above, insurance is an important tool in every CFO's risk-mitigation toolkit. That's why every company should theoretically carry some sort of cyber insurance policy to protect it against the financial losses associated with a cyberattack or other technology-related hazard.

But getting the right cyber insurance coverage for the right price is easier theorized than done. Insurers in recent years have found themselves paying too many claims for too much money too often. So they're significantly adjusting their underwriting standards accordingly.

As a result of these increasingly stringent underwriting standards, cyber insurers may:

- **Deny companies coverage outright** if they fail to meet their new, higher standards for security diligence.
- **Deny paying damage claims** if they discover after the fact that a policyholder was not fully implementing all the measures and controls specified in their agreed-upon terms of coverage.
- **Bring legal action against policyholders** if they believe that representations the policyholder made regarding their cybersecurity posture were not wholly accurate.

These contingencies dangerously undermine a CFO's ability to mitigate their organization's cyber risk with cyber insurance.

Financial Impact 4

Legal and regulatory exposure

Insurance companies aren't the only stakeholders that can take a company to court as the direct consequence of a cybersecurity breach. A growing number of law firms specializing in cyberlaw are aggressively filing class-action lawsuits against companies on behalf of customers who have been affected by data breaches.

The financial judgements resulting from these lawsuits are sobering. They include judgements against Equifax ($380 million), Home Depot ($200 million), CapitalOne ($190 million), and Uber ($148 million). And, again, smaller companies aren't immune. Their losses will simply be proportional to their size and the number of customers involved.

Companies subject to regulations such as PCI (for credit card data), HIPAA (for healthcare information), or SEC guidelines (for financials) can face legal consequences from the associated government agencies as well. In addition, regulators who find that a security breach was the result of managerial negligence can take the further step of imposing Code of Conduct restrictions on the offending company. And those restrictions can seriously hamper a company's ability to sell certain types of products or participate in certain markets.

Financial Impact 5

Supply-chain disruption

The financial risks associated with cybercrime extend beyond a company's four walls to its suppliers, contractors, and other business partners. That's because a company's ability to do business is not only jeopardized by the possibility of an attack on its own digital infrastructure. It's also jeopardized by the possibility of an attack on a key supplier.

If such a supplier is hit with a cyberattack and therefore cannot deliver whatever it is expected to deliver—whether material, components, finished goods, services, or information—**the affected company can still suffer many if not all of the financial impacts associated with an attack on its own digital environment**.

Furthermore, many cyberattacks readily spread via digital "contagion." An infected supplier thus not only threatens its customers indirectly through a failure to supply. It can also serve as a useful launching pad for an attacker to successfully infect that supplier's customers.

Conversely, a customer who suffers an attack can adversely impact a supplying company in two similar ways. First, the paralyzed customer may cancel current orders and fail to place any new ones—thus costing the supplying company substantial revenue. This risk is especially significant if the supplying company receives a large percentage of its revenue from a small number of key accounts.

Second, just like an infected supplier, an infected customer may serve as a launching pad for an attack on the supplying company.

Collectively, these five under-recognized financial risks —plus the well-recognized risk of extended business downtime—represent dangers that every CFO must identify, analyze, quantify, and address. **Failure to do so can imperil the future of the organization they are charged with protecting.**

A plan of action

Risk management is a complex discipline. So it's clearly beyond the scope of this brief report to describe in detail all the actions, decisions, and processes CFOs must put in place in order to optimally protect their organizations from the financial risks associated with cybercrime.

However, three basic steps are essential for every CFO seeking to effectively address their organization's cyber risks sooner, rather than later:

Step 1

Catalog and size the risks. This report offers an excellent starting point for cataloging and sizing the potential adverse financial impacts today's intensifying cyber criminality can have on organizations that are increasingly dependent on technology. That catalog will provide a sound basis for determining mitigation strategies, allocating resources, and communicating with other stakeholders.

And CFOs should abide by the time-tested principle to not allow the perfect to be the enemy of the good. A reasonably useful catalog being used today in practice is of infinitely greater value than a precisely accurate catalog that doesn't yet exist—and probably never will.

Step 2

Get a third-party assessment of current exposures to cyber risk. No one manages risk to their physical health by just going to the pharmacy and getting every medicine available. Instead, they go for a medical checkup to see where they are at risk and where they are not.

The same principle holds true for managing cyber risk. Every CFO should get a cyber risk checkup for their organization. And that checkup should be performed by a qualified independent third party—because internal IT departments cannot check their own work, and cybersecurity solutions companies are too predisposed to turning every company they assess into a nail for their particular hammer.

Step 3

Create a team and a process. The battle against cyber risk is an ongoing one. That's because every company's risk profile changes as it implements new technologies, as it hires and fires employees, as it does business with an ever-varying cast of customers and suppliers, and as the tactics of cybercriminals continue to evolve.

Effective risk management therefore requires periodic updating of the risk catalog, regular third-party risk assessments, and close communications with all stakeholders in the mitigation of technology-related risk—including IT, legal, key suppliers, and others.

vCSO Magazine

vCSO Magazine provides executive decision-makers with actionable, high-value insights into the risks and opportunities they face in today's increasingly digital global marketpace.

info@vCSOMagazine.com | (615) 922-6777 | 342 Harrison St. Nashville, TN, 37201

