Recorded Future®

Cyber Security Case Studies

DIGITAL (IT) GOVERNANCE IS BROKEN!

9 Ways Enterprises Mismanage Their Cyber Risk

By Courtenay Brammar and Levi Gundert

Introduction

The fallout from the Solar Winds breach[1] is the latest example of the huge costs and consequences that can result from a cybersecurity event; however, these types of cyber events are not outliers. As mainstream headlines now report, expensive cybersecurity events are only accelerating irrespective of organizational size, geography, or industry.

In our experience, as cyberattacks increase in complexity, frequency, and velocity, many enterprise organizations rely on outdated IT governance. The organizational paradigm is limited by slow-moving bureaucracy and scarce resources. This situation is often the result of a limited understanding of decision-makers' risks, like board executives who rely on outdated corporate governance frameworks developed in response to accounting scandals (like WorldCom, Enron, or Tyco), not cyber risks.

Enterprise executives continue to propagate a compliance check-box mindset that values minimal security control investment to meet audit standards. The focus on audit and compliance misses the costs that may extend beyond regulatory penalties into financial losses that are not always small enough to recover without significant repercussions.

In this paper, we draw from consulting experience, candid conversations with security leaders, and empirical research to define the nine issues currently plaguing enterprise cyber governance, while offering remedies for organizational leaders striving for a useful governance model that moves beyond audit compliance to iterative and measurable risk reduction.

[1] https://www.bloomberg.com/news/articles/2020-12-21/solarwinds-adviser-warned-of-lax-security-years-before-hack

Dysfunctional IT Governance, Let's Count the Ways

The specifics of digital governance may vary, but a generally accepted definition[2] is: "the process of specifying the decision rights and accountability framework to encourage desirable behavior in the use of information technology". Internal governing bodies, management, and audit all play vital roles in successful governance.

Synonyms for governance include authority, control, power, influence, administration, jurisdiction, rule, and government. The decision-rights aspect of governance is relatively straightforward when chartered appropriately. However, "encouraging desirable behavior" in cyber risk management, as a subset of information technology, is where organizations need to improve substantially.

1. **Security spend decision-making in most large enterprises is generally conducted by a committee, which is a slow, consensus-driven process.** There are four ways that cyber risk is escalated to an enterprise relevant committee:
    1. Self-identified by the business unit via internal risk assessment
    2. Identified proactively/reactively by the CISO/InfoSec team based on external or internal events
    3. Escalated via an Audit action point identified in their review (often after an issue materialized prompting the review)
    4. Highlighted by a regulator's finding (who are naturally reactive)

There is a contradiction in the prevailing cyber governance approaches and cybersecurity spend allocation. The way that concerns get raised to decision-makers in committees is at odds with the cyber paradigm because when it's apparent that risk is materializing, quick decisions about considerable spending are sometimes required to correct the underlying vulnerabilities or mitigate the risk.

For example, in May 2017, had Maersk immediately performed thorough financial modeling or scenario analysis exercise using the National Health Service's large-scale disruption caused by cyberattackers earlier that month (which was a result of an exploited vulnerability and aged tech) as the basis for a reasonably realistic scenario, could they have presented their analysis to the board of directors swiftly enough through existing corporate governance mechanisms to compel spending $205 million on technology controls and avoid $110 million in lost revenue by late June?

Doubtful. Budget committees tend to meet only at regularly scheduled intervals due to the seniority of those involved plus the time required for meeting content production, so it would've been difficult to get their analysis in front of a committee for a decision.

[2] https://www.researchgate.net/publication/236973378_IT_Governance_How_Top_Performers_Manage_IT_Decision_Rights_for_Superior_Results

A common misconception is that scenario modeling increases certainty about a problem, meaning it's expected to provide the answer, whereas the reality is that it only reduces uncertainty, meaning there is still a judgment to be made.

It's difficult to know where companies like Maersk stand in terms of audit compliance prior to the cyber events that result in financial loss. However, each of the initial access categories used in these events is preventable or discoverable through recognized security controls. These events are the short list[3] reminders that compliance does not equal risk management beyond Audit.

2. **Outdated governance models propagate security control spending inertia.** The ever-present burden is on CISOs to determine not just how much their enterprise should expect to spend on security but also convince their governance functions to approve the spend. The penalty for inaction may be considerable financial losses, but many organizations are still playing Russian roulette with deferred investment.

Consider Unicredit. Unicredit disclosed that between 2015 and 2019, multiple security incidents affecting 4.1 million Unicredit customers cost the bank over $2.8 billion ($679 per victim customer) in cybersecurity control improvements. Digital governance decisions are made based on an inaccurate view of cyber insurance coverage. Insurance may cover partial losses, but it won't cover all of them, and, more importantly, it can't repair a reputation in tatters after a devastating public attack. A realistic appreciation of "value at risk" is rarely supplied to executives.

Recently deployed techniques suggest that threat actors are wise to organizational constraints around cyber decision-making:

- An English football club was victimized[4] by a 2020 ransomware attack where turnstiles were halted by attackers demanding a ransom.
- In July 2020, a mischief-making cyberattack — where there seems to be no other purpose than to show the ineptitude of management — victimized UFO VPN[5].

Threat actors are also known to exploit transparency disclosures — another stalwart of corporate governance — by doing the following:

- Targeting relevant companies with business email compromise after public disclosure of key executive(s) leaving. In May 2015, Ubiquiti Networks lost[6] $39.1 million to a BEC scam shortly after the resignation of their chief financial officer in April.
- Using public year-end financials/quarterly forecasts to identify victims and determine how much ransom to demand from them ("darkside threat"). In July 2020, Carlson Wagonlit[7] suffered a ransomware attack where threat actors had initially demanded $10 million and only after negotiation (details of which were made public on Twitter) accepted a mere $4.5 million.

When to spend? Should organizations wait until they have to pay out in response to a breach or a ransomware attack, or proactively invest? Under-investment may have played a role in Unicredit's outsized spending, for example. In 2019, JP Morgan reportedly spent $600 million annually on cybersecurity, up from $250 million just five years prior.

[3] https://oag.ca.gov/privacy/databreach/list
[4] https://www.zdnet.com/article/ransomware-attack-locked-a-football-clubs-turnstiles-almost-leading-to-cancelled-match/
[5] https://www.hackread.com/hackers-destroy-ufo-vpn-database-meow-attack/
[6] https://www.tripwire.com/state-of-security/latest-security-news/bec-scam-results-in-39-1-million-loss-for-ubiquiti-networks/
[7] https://www.reuters.com/article/us-cyber-cwt-ransom/payment-sent-travel-giant-cwt-pays-4-5-million-ransom-to-cyber-criminals-idUSKCN24W25W

Would auditors ever suggest an approach like this and present these numbers? It's doubtful. One of the most fundamental issues with the current corporate governance approach is that decisions are made with an entirely too conservative frame of reference — fiscally, technologically — and for many boards of directors, cybersecurity investment beyond compliance mandates still represents a leap of faith.

The budget-keeping mindset for cybersecurity misses this fact that the costs are not solely financial and are not always small enough to recover from without significant repercussions, and not just in the digital realm. Entire enterprises have closed because of the losses incurred by a cyberattack[8]. People have died because of cyberattacks.[9]

Most recently, the considerable increase[10] in remote work due to the COVID-19 pandemic has added to most enterprises' difficulties in bringing immediate security concerns into sharp focus.[11] Control gaps due to remote work should be addressed immediately, especially given that many employees will likely wish to continue working from home even after the pandemic ends.

3. The CISO (chief information security officer) reports to the CIO (chief information officer). **This reporting structure creates misaligned incentives between the technology enablement mission and reducing operational risk.** A former security operations manager summed up his experience in a Fortune 500 company as, "remediate security incidents as quickly as possible to avoid the information ever escalating to the CIO".
4. **Organizational charts do not equal good governance.** Traditional enterprise organizational structure rarely facilitates good governance. Governance, risk, and compliance (GRC) groups and operational security groups are misaligned for optimal risk assessment and communication. Interviews with GRC professionals reveal the perception that GRC is only concerned with passing audits (like SOX, SOC 2) while operational security teams are aloof and lack the patience to explain technical security concepts or strategies. The division in reporting structures exacerbates the problems.
5. Compliance efforts contribute to successful audits, but **compliance does not directly correlate to operational risk reduction**. Correctly identifying, measuring, and communicating risk to executive stakeholders takes a backseat to compliance progress. Over time enterprises prioritize a "check the box" mentality while success is defined as increasing maturity model scores. Security controls are prioritized for passing audits to the detriment of risk management.

   Unfortunately, in the case of technical security controls, good compliance results in successful audits, but not necessarily reduced risk. This is because cyber threats appear and evolve daily, sometimes by the hour, while compliance frameworks update much slower and less frequently — typically every 18 to 24 months, sometimes longer. The past decade is littered with companies that suffered a breach after passing an audit and being certified compliant.
6. **CEO detachment from cyber risk management is a digital governance issue.** Gartner expects that by 2024, "75% of CEOs will be personally liable for cybersecurity incidents[12]". As CEOs become personally liable, their potential removal from the company causes negative impacts. For example, in 2020, the Finnish psychotherapy center Vastaamo suffered a data breach[13] that led to extortion and the CEO, Ville Tapio, being fired.

[8] https://threatpost.com/hacker-puts-hosting-service-code-spaces-out-of-business/106761/

[9] https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/

[10] https://www.news.com.au/technology/online/hacking/remote-workplaces-create-perfect-system-for-hackers-as-cyber-attacks-on-the-rise-experts-warn/news-story/39f0227d3b63f3099075cb21e5b9c152

[11] https://securityboulevard.com/2020/08/covid-19-reveals-the-dirty-truth-about-security-spending/

[12] https://www.gartner.com/en/newsroom/press-releases/2020-09-01-gartner-predicts-75--of-ceos-will-be-personally-liabl

[13] https://www.helsinkitimes.fi/finland/finland-news/domestic/18234-is-vastaamo-fires-ceo-saying-he-knew-about-hacking-for-18-months.html

7. **Enterprise executives often make poor control investment decisions based on bad data** as they attempt to define a degree of relative risk urgency based on qualitative assessments. Based on current controls, not every cyber threat poses a risk.

   Risk self-assessments by first-line or business teams involve first identifying the team's risks, then assessing them, before mapping them to controls, re-assessing them in consideration of the control environment, and completing the exercise by adding them to a risk matrix for reporting purposes.

   A common misconception about managing cyber risks is that every threat identified needs to be fixed. This is simply impossible (or more precisely, requires an investment of resources that can be financially impractical to scale).

   Separately, a loss scenario that is less costly than implementing a new control must be designated as an accepted risk — ideally with a justification.

   The risk assessment aspect for business teams tends toward using a "qualitative" approach to assessing each risk because risk quantification is hard or "technical". This means assessing the risk by applying a traffic light (red/amber/green) rating (which adheres to a definition likely devised by the enterprise risk team) to each risk based on their probability and likelihood. Each risk is then depicted on a "risk matrix" to help visualize their team's risks.

   Some criticize this approach for oversimplifying risk management, because sometimes two risks feel considerably different (better/worse), but when using the "traffic-light" methodology, they end up in the same matrix box, leaving some business teams genuinely dissatisfied with the whole process of risk self-assessment.

   Risk teams and the rest of the business, particularly the auditing groups that unintentionally act as gatekeepers for risk and control identification in many organizations, may not interpret risk the same way. This leads to two approaches that commonly play out among business teams when assessing their function's risk across enterprises:

   1. "Once that security event materializes, I'll get the budget I requested" — a reactionary approach that risks waiting for a security event to potentially cause great harm before the team is able to get the resources needed.
   2. "If I self-identify within the risk assessment, they might expect me to solve the issue without additional budget. Whereas if I wait for Audit to find it, I'll get the extra budget, and if Audit misses it, how could we have known about it?" This approach simply pushes the problem down the road.

Both problems arise from the disconnect between the people in an organization who directly deal with cyber issues and the people responsible for managing and budgeting for those teams.

After the satisfaction derived from the sense of "getting your arms around" your risks and controls by identifying and assessing them, it's often the case that once you apply them to the risk matrix you find yourself in an uncanny valley scenario described by Phil Venables[14] (In short, Venables argues that there is generally a point where teams get good enough at assessing risks that they realize the greater scope and complexity of the issue and go from previously rising levels of confidence to a steep dropoff of disillusionment).

[14] https://www.philvenables.com/post/the-uncanny-valley-of-security-or-why-we-might-never-finish-anything

8. **A collective owner approach ("everyone is an owner") to digital governance leads to an expanded attack surface** increasing the risk of cybersecurity events and financial loss.

The collective ownership approach to cyber governance includes four distinct roles:

- **Preventative —** For example, not clicking on an email supplied phishing link
- **Detective —** For example, identifying suspicious activity like files being opened by someone who doesn't have a business need for them, and then escalating the observation
- **Corrective —** For example, resetting passwords after a cyber event/near miss
- **Directive —** For example, rewarding individuals within their team for practicing good security hygiene

The problem with this approach is that when every employee is on the front lines, each employee is also effectively an asset to threat actors. When everyone has their own phones and computers connected to the company network, they each individually become targets for attacks like phishing attempts and other forms of business email compromise, or simply present access points into a network that may be leaked through third-party data breaches, as in the case of the Blackbaud leak. With a vastly expanded threat surface where every employee represents a potential point of failure, victimization is inevitable.

Blackbaud, a cloud services provider, adopted the collective ownership approach before being victimized in 2020 by a breach that impacted over 20 million people. The breach resulted in derivative extortion attacks.

9. **Excel spreadsheets and additional headcount may be reasonable for a proof-of-concept risk register, but it's a woefully insufficient solution for tracking the state of cyber risks and corresponding controls.** In an interview with a longtime GRC veteran, she described outsourcing a risk/controls identification exercise. The consulting group identified critical business processes and returned with 900 controls to implement, before reducing the list to 256 controls to satisfy audit regulatory requirements.

Nine Solutions

1. Enterprises must consider an alternative approach for cyber resourcing decisions that extend beyond audit compliance. **Ideal digital governance requires management and budget committees to have visibility into both audit compliance and IT risk management to properly allocate cybersecurity resources.**

We discussed the negative impacts of solely focusing on audit outcomes, but the audit function does occasionally provide value beyond compliance. For example:

- In April 2018, weak authentication credentials at Erie County Medical Centre[15] resulted in a ransomware attack. The medical center was relieved to have taken heed of their auditors' suggestion to increase cyber insurance coverage five-fold (from $2 million to $10 million) prior to the ransomware attack, which would have left them $8 million out of pocket.
- In November 2020, the Folksam Group[16] disclosed that they had been accidentally allowing technology companies to access customers' private data. Folksam Group's internal auditors uncovered the unauthorized access.

Put simply, satisfying audit requirements is obviously important but so is identifying and managing cyber risks that exceed audit visibility.

Cyber threats evolve daily, so control validation should be occurring weekly, if not daily. A quarterly penetration test is sufficient for audit requirements but insufficient to address changing adversary tactics. Quick decisions about security spend are often required to mitigate unacceptable risk. These quick decisions must be made by quickly and accurately interpreting very technical information, often large volumes of it. Reducing that technical information down to befuddling dots on color-coded matrices doesn't create efficiencies — it wastes resources.

In our experience, the operational risk from cyber events, represented as financial loss, is not well understood by enterprise C-suites and boards of directors. Improved quantitative techniques[17] are required to convert poor quality data in a "likelihood of occurrence times impact" equation with traffic light and heat map outcomes into annual loss amounts with attached probabilities that account for the unknown.

2. **Provide solid data justifying proactive spending**, such as through analyzing the cyber experiences of other organizations.

[15] https://buffalonews.com/business/local/ecmc-spent-nearly-10-million-recovering-from-massive-cyberattack/article_1786edc7-2e-5c48-84c5-8823a2a38e91.html
[16] https://www.bleepingcomputer.com/news/security/folksam-data-breach-leaks-info-of-1m-swedes-to-google-facebook-more/
[17] https://www.amazon.com/Risk-Business-CISOs-Risk-Based-Cybersecurity/dp/1948939134/

Consider the table below, derived from publicly available data:

Initial Access Category[18] ("Left of Boom")	Post-Compromise Category ("Right of Boom")	Loss Details	Company	Occurred	Amount
Social Engineering / Phishing	Destruction of Data or Systems Availability	Control Environment Improvement/ Crisis Management	Maersk	Aug 2017	$300 million
Social Engineering / (Possibly Phishing)	Destruction of Data or Systems Availability	Crisis Management / Forensic Investigators	Sony Corp.	Dec 2015	$15 million
Social Engineering / (Possibly Phishing)	Destruction of Data or Systems Availability	Control Environment Improvement / Crisis Management	Sony Corp.	Mar 2016	$20 million
Credential Reuse	Theft of Employee or Customer PII	Ransom Payment	Uber Inc.	Oct 2016	$100,000
Credential Reuse	Theft of Employee or Customer PII	Control Environment Improvement / Restitution	Uber Inc.	Sep 2018	$148 million
Compromised Credentials of Connected Third Party	Theft of Employee or Customer PII	Regulatory fine	British Airways	Sept 2018	$26.7 million
Social Engineering / (Possibly Phishing)	Destruction of Data or Systems Availability	Insurance	Sony Corp.	Jan 2015	$35 million
Web Application Vulnerabilities	Theft of Employee or Customer PII	Regulatory Fine / Cnil fine	dailymotion.com	Aug 2018	$60,000
Credential Reuse	Theft of Employee or Customer PII	Regulatory Fine / Dutch DPA fine	Uber Inc.	Nov 2018	$735,000
Credential Reuse	Theft of Employee or Customer PII	Regulatory Fine / France's DPA fine	Uber Inc.	Dec 2018	$490,000
Credential Reuse	Theft of Employee or Customer PII	Regulatory Fine / UK's ICO fine	Uber Inc.	Nov 2018	$525,000

Looking specifically at the remediation costs of other companies that suffered data breaches:

- In 2019, 106 million Capital One customers were affected by a data breach, and according to one estimate, the event could cost them $500 million, or $4.72 per victim customer.
- In 2019, 33,000 customers were impacted by a breach at DSK Bank that resulted in a fine levied of $569,930 (1 million Bulgarian levs), or $17.27 per victim customer
- In November 2016, the U.K.'s Tesco Bank suffered a "cyber bank robbery" after the data of 40,000 customers was breached, costing them at least $26 million, or $627.50 per victim customer.

[18] Categories extracted from https://cyber-edge.com/wp-content/uploads/2020/06/Recorded-Future-The-Risk-Business.pdf

One caveat is that this data set necessarily only includes companies that have publicly disclosed these figures. But even from these three examples, we see that the cost per customer can be anywhere from a few dollars to many hundreds of dollars — a figure that becomes hugely costly when data breaches regularly affect many hundreds of thousands or millions of customers.

We're advocating for using a financial modeling approach to risk quantification to push through the uncanny valley (see point 7 above) and reach a place that continues to gather momentum through its measurability over time.

Financial modeling has almost exclusively been put to good use in the enterprise risk management space for capital adequacy purposes — that is, to determine the amount of capital an enterprise should have to set aside for their operational liabilities.

Enterprises should use financial modeling approaches, like annualized loss expectancy,[19] for cyber risk quantification to ascertain the justification of cyber control spend using external data from real-life events to determine the parameters across the potential exposure of a given threat and the control cost estimate.

3. **The CISO should be a peer of the CIO.** To align effort effectively, GRC and operational security teams should both report to a chief risk officer (CRO), chief operating officer (COO), or chief financial officer (CFO). Enterprises generally tuck the chief information security officer (CISO) under the chief information officer (CIO) because the responsibilities all have a vague nexus to technology. That's a mistake. When a CISO reports to a CIO there may be objective misalignment. Additionally, the CISO may be missing a proverbial seat at the senior executive table.
4. **Align incentives and motivations between GRC and operational security teams** to help increase mutual respect for each other and for the overarching objective of digital risk management. In interviews with both longtime GRC and security operations practitioners, it quickly became clear that these groups do not generally collaborate, but rather are constantly reacting to perceived criticalities, generally instigated by an audit.

   GRC is concerned with control framework maturity, but they often lack the resources to perform control assurance properly. A GRC group may be tasked with identifying critical business processes, implementing controls (typically hundreds), and satisfying regulatory requirements by way of internal and external audits.

   Operational security teams, on the other hand, are tasked with micro-monitoring controls and remediating cybersecurity events as necessary. The workflow is often a fire drill of responding to new software vulnerabilities with patching routines, malicious code (malware) infections, password resets, and the addition of new indicators of attack/compromise to firewalls, web proxies, and network/host-based security appliances.

   One caveat is that IT groups must continue to support information assurance functions with necessary tools and resources, regardless of the security team reporting structure. For example, Security Operations often requires access to a SIEM (for example, Splunk) for security device log analysis. If IT drags their feet provisioning accounts or allocating necessary storage, Security Operations is less effective.

[19] https://en.wikipedia.org/wiki/Annualized_loss_expectancy

5. **Executives and the board of directors need two real-time views: audit compliance and risk management.** Passing audits is obviously important to avoid regulatory penalties or worse. Enterprises pour significant resources into compliance to avoid sustained audit headaches. GRC frameworks are numerous and complex. Improving maturity against any one technology framework, let alone multiple, is an onerous task requiring significant resources, that often still results in unidentified control gaps. The acronyms alone are dizzying — COBIT, Risk IT, NIST SP800, ISO 27001/27002, HIPAA, PCI DSS, APQC — when attempting to map, tailor, and meet the requirements.
6. Beyond compensating for personal liability, **more CEO engagement in digital governance is important to organizational success.** A few recent positive examples of CEO engagement include the following:
    - In 2018, Hancock Health's CEO published his own account[20] of an attack after threat actors obtained the login credentials of a vendor providing hardware for one of the hospital's information systems.
    - Reporting cyber near-misses is becoming more commonplace[21]/acceptable[22]. This is a good sign; it's important to celebrate the wins, not only commiserate the losses. It can be a gamble, however,[23] taking the PageUp breach, some of their customers, like Aurizon Holdings, disclosed[24] the "near miss", and then some had to follow up with a more dire impact assessment.
7. **For that subset of threats that do need to be managed as risks, the next steps are to triage them and then resolve them — as through a risk register.** The act of triaging — assessing the degree of relative urgency — is subjective. Intelligence becomes a necessary requirement to differentiate adversary tactics and compare their impact to existing security controls. Compliance gaps are easier to identify with a framework. Operational security risk that exists between controls, and in controls, are less apparent without strong intelligence.

    A loss scenario that is less costly than implementing a new control must be designated as an accepted risk — ideally with a justification.

[20] https://www.hancockregionalhospital.org/2018/01/cyber-attack-pov-ceo/
[21] https://mexiconewsdaily.com/news/bank-acknowledges-attempted-cyberattack/
[22] https://alumni.utoronto.ca/news-and-stories/news-and-articles/message-our-community-recent-blackbaud-data-breach
[23] https://www.aurizon.com.au/news/news/unauthorised-access-of-third-party-vendor-it-systems
[24] https://www.aurizon.com.au/news/news/update-unauthorised-access-of-third-party-it-vendor-system

8. A collective governance approach demands resources to ensure a high degree of security awareness and education. **Employees need to be informed and empowered to act well beyond the scope of traditional compliance training.** Creating compelling training that improves security in employees' personal lives will also benefit the enterprise.

   The alternative is carefully considered overt and covert surveillance of employee activities, which diminishes trust across a company and is counterproductive to collectively motivating employees to help detect and subvert cyberattacks.

9. **A near-real-time unified view of GRC and operational security risk underpins good digital governance.** Boards of directors should have access to the same dashboard as managers and be less reliant on point-in-time presentations. If the authority and responsibility to make relatively quick security resourcing decisions to address new risk is in place, then data visibility speed is the final ingredient for success. **To continuously validate large numbers of security controls and present quantitative loss figures requires substantial automation.**

   An operational security director recently shared his experience with a distributed denial-of-service (DDoS) attack that impacted his company's e-commerce revenue. Following the attack, there were internal questions such as, "What does this type of attack cost the company?", "How much does a new control cost to mitigate these types of attacks in the future?", "What is the probability that this type of attack occurs again this year?" "How often this year?" "Do we need a business process change?" Without automation, these questions take too long to answer. Real-time risk views ensure stronger governance.

Upending the Status Quo of Digital Risk Management

Digital risk management is a moonshot in the context of enterprise technical complexity and adversaries with near-limitless resources and focus.

Enterprises that wish to have a fighting chance must implement good digital governance:

- First, enterprises must consider an alternative approach for cyber resourcing decisions that extend beyond audit compliance, for example, cyber threats evolve daily and continuous control validation — far beyond audit requirements — is necessary to understand operational security control gaps that require attention and often resources.
- Second, enterprise committees must overcome spending inertia on operational security that addresses risk beyond Audit. To improve, decision makers must have quality data justifying proactive spending, such as through analyzing the cyber event losses of other organizations.
- Third, the CISO should be a peer to the CIO.
- Fourth, align GRC and operational security in the same organization with similar incentives.
- Fifth, management and executive committees need updated views into both audit compliance and digital risk management, and not assume they are one and the same, they are different.
- Sixth, CEOs must increase engagement in digital governance and risk management.
- Seventh, cyber risk must move from qualifications to loss quantifications to ensure resource decision-makers are correctly informed.
- Eighth, the CISO should own the responsibility, authority, and resources — in a collective ownership approach to security — to properly educate employees to actively participate in the defense, and also protect employees in the process.
- Ninth, the combined visibility requirements for enterprise GRC and operational security functions are enormous. Automation technology must play a critical role in aggregating, analyzing, and presenting top-level cyber risk metrics.

Changing the enterprise digital governance paradigm is difficult, but the status quo of focusing on audit compliance with an insurance policy safety net is short-sighted.

Enterprises will continue to be individually and opportunistically targeted by adversaries that can impose losses beyond regulatory fines and insurance[25] deductibles. Now is the time to rethink digital governance and the variables that underpin it.

[25] https://hbr.org/2021/01/cybersecurity-insurance-has-a-big-problem

Courtenay Brammar is Director of Risk Analysis and Insights at Cyber Security Case Studies.
She lives in Europe.

Levi Gundert is the SVP of Global Intelligence at Recorded Future.
He lives in Southern California.