eSENTIRE

UHY Consulting

Cybersecurity Governance for Small and Medium Businesses

Building a Foundation to Enable Informed Decisions

Table of Contents

Executive Summary

Today's small and medium businesses (SMBs) are subject to a wide array of cyberthreats and are particularly vulnerable because they don't have the same resources as enterprises and other large organizations.

Empirical research demonstrates that it's only a matter of time before an SMB suffers a cybersecurity incident. And the consequences can be dire: for instance, data breaches can cause staggering losses, significant regulatory penalties and permanent harm to an organization's reputation and competitiveness.

While cybersecurity is a complex, multi-disciplinary topic, SMB decision makers nevertheless require a fundamental understanding of the cybersecurity domain and a risk management plan as it relates to their business. Board members do not need to become IT experts, but they must know what questions to ask the Information Security and Information Technology (IS&IT) departments.

Additionally, boards must provide the leadership and commitment necessary to make protecting the organization a priority. Part of this leadership is knowing and championing the five pillars of cyber risk management: awareness, risk, program, reporting and incidents.

Enabling cybersecurity governance requires an effective governance structure, board visibility into the right metrics and an appreciation of the relative dynamism of security needs.

The most effective SMB governance structures come from a combination of top-down principles that define the objectives and operational approach of a complementary bottom-up effort. Importantly, the board needs to recognize the flaws and trade-offs inherent within any reporting structure and consciously advocate for an approach which will provide them with the information and visibility they need.

Metrics have maximum value when they capture an operating reality and can be placed in context. When these conditions are met, metrics reveal how you are performing today and how your performance is changing over time in the operating context of your business and risk environment. These insights enable the board to make decisions which help the business get to (or remain in) a desired state.

When it comes to cybersecurity, most SMBs need to adjust their thinking regarding operating timeframes. Often, this thinking is shaped by annual planning cycles and long-term horizons, which is too slow to keep pace with the changing capabilities of modern threats. Likewise, the organization must be able to execute with velocity: there's little point in quickly making the correct decision if teams don't have the resources to take action.

Finally, to understand and govern an SMB's cybersecurity program, it's convenient to divide the broad subject into separate knowledge domains: situational awareness, strategy and operations, insider threats, incident response capabilities and supply chain/third-party risks. This separation breaks a complex domain into manageable pieces.

Ultimately, managing cyber risk comes down to making informed decisions which balance risks and costs. Often, the most suitable approach for a small or medium business is to work with external security operations partners who can provide expertise, fill skill gaps and consult on how best to implement and manage a cybersecurity governance program.

Introduction

Corporate governance ensures a company conducts itself accountably, fairly and openly in all its dealing, according to the six principles of fiduciary care. It manifests as a collection of controls, processes and reporting mechanisms, aligned to specific business goals and industry regulations.

Governance is the responsibility of a company's board of directors and, when effective, enforces accountability and fairness, provides transparency, delivers assurance and protects investors and stakeholders. Most importantly, it displays leadership and sets the tone from the top.

Risk management is intertwined with governance, as businesses must balance potential gain with the risk associated with pursuing defined goals. While financial management and legal compliance receive most of the attention, cybersecurity has quickly gained prominence as a key element in the risk management equation due to the profound and unprecedented operational, financial and legal consequences involved.

Threats facing today's organizations

Today's organizations are subject to a wide array of cyber threats. From opportunistic attacks using commodity malware as a service, to sophisticated hands-on-keyboard attacks which surgically evade defenses, to advanced persistent threats which can operate for years undetected, to industrial espionage using legitimate credentials harvested from phishing campaigns—the list is long and the consequences can be devastating.[1]

As businesses adopt cloud-based services and employ a distributed workforce, this always-connected model increases the attack surface—the collection of points a malicious actor can use to try to gain access. The COVID-19 pandemic has amplified this threat, with malicious actors opportunistically focusing malware and phishing activities on remote working technologies and pandemic-related lures.

This broad trend has played out for organizations of all sizes, but has left SMBs particularly vulnerable. SMBs generally don't have access to the same resources and expertise as their enterprise cousins, and the unfortunate result is that their security posture—the overall security status of their software and hardware, networks, services and information—has failed to keep pace with either the expanding threat surface or the ongoing evolution of the threats.

While cybersecurity is a complex, multi-disciplinary topic, today's decision makers within SMBs require a fundamental understanding of the cybersecurity domain and a risk management plan as it relates to their business.

To protect against the myriad of attacks that already exist and which continue to be developed, security initiatives must be prudent and practical. This is where risk management comes into play within the larger domain of responsible corporate governance.

It's not the responsibility of the board to become IT experts, but the board must know what questions to ask the Information Security and Information Technology (IS&IT) departments. Additionally, boards must provide the leadership and the commitment necessary—by proactively overseeing and holding management and the C-suite accountable—to make protecting the organization a priority.

[1] For a snapshot of the contemporary threat environment, see eSentire's 2019 Annual Threat Intelligence Report

Pillars of risk management

There are several good guides on the key pillars of risk management and board obligations, including The National Association of Corporate Directors (NACD) Cyber-Risk Oversight Guide,[2] the National Cyber Security Centre Board Toolkit[3] and Navigating the Digital Age.[4]

While each resource provides differing levels of information, there are five common pillars:

- **Awareness:** Understanding the impact of cyber risks and trends, experiencing the business impact of a breach and exposing personal risks
- **Risk:** Identifying non-public assets and protected data, and documenting regulatory and contractual obligations
- **Program:** Establishing budget, staffing and programs that align to overall business risk priorities
- **Reporting:** Annual planning, quarterly reporting, dashboards and peer/industry comparisons of performance
- **Incidents:** Understanding incident response, board roles, critical business decisions and reporting to authorities and crisis communications

[2] https://www.nacdonline.org/insights/publications.cfm?ItemNumber=67298

[3] https://www.ncsc.gov.uk/collection/supply-chain-security

[4] https://www.securityroundtable.org/navigating-the-digital-age-2nd-edition

Quantifying the Risks

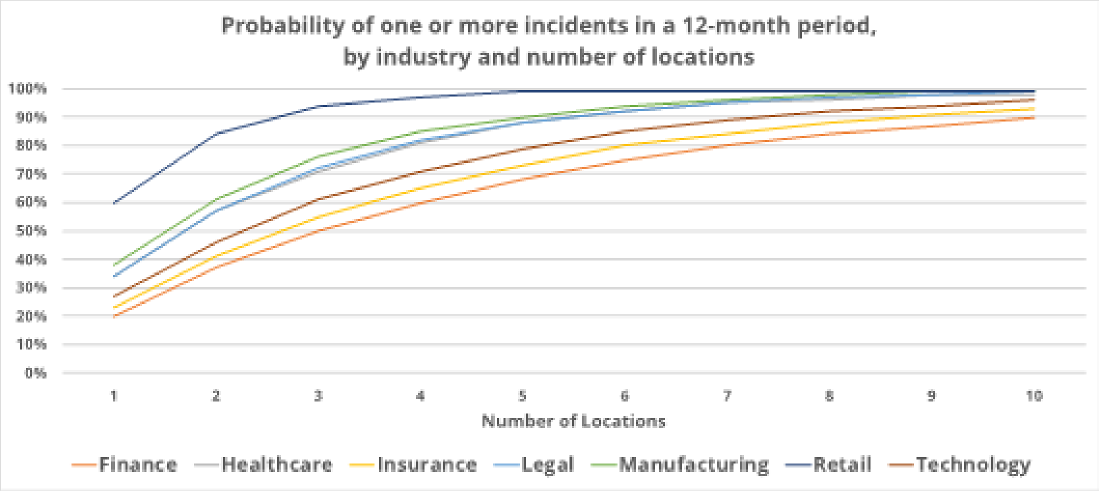
In the 2018 Ponemon State of Endpoint Risk Study, 64 percent of survey respondents indicated that their organizations suffered a data asset and/or IT infrastructure compromise, reflecting a 54 percent increase over the previous year. Of those breached, 57 percent reported significant disruption to business operations with a loss of more than 1,000 records containing sensitive or confidential information.[5]

Of course, one limitation of relying on a survey is that only respondents who know they have been compromised can indicate that a compromise has occurred. This sample bias means that the Ponemon stats undercount security incidents because many compromises go undetected.

It's not a matter of if, but when

The most accurate way to inform predictions about risk is to study the real world. Using observational data from our Security Operations Centers (SOCs), eSentire calculated the mean probability that an organization had at least one incident involving a bypass of existing endpoint security controls, in a 12-month period.

While the degree of risk shows some variation by industry, the conclusion is clear: it's only a matter of time before an organization suffers a cybersecurity incident. Even small businesses with a single location can realistically expect to face at least one incident every two years.[6]



[5] Ponemon: 2018 State of Endpoint Security Risk Study

[6] And note that the figure is limited to bypasses of endpoint security controls; that is, it doesn't even account for network or cloud intrusion, impersonation attacks and other threats

Not all cyberattacks are created equal

It’s also important to recognize that security incidents vary in impact and consequences. Some may create relatively minor inconvenience while some may lead to staggering losses. Severe incidents may result in significant regulatory consequences or permanently harm an organization’s reputation and competitiveness.

Often, cyberattacks are classified by severity as events, incidents or breaches:

- **Events** include minor issues with no impact to business. This could be a simple as a firewall or endpoint protection blocking an unauthorized attempt to connect to the network or preventing malware installation
- **Incidents** are more serious and relate to violations of the firm’s cybersecurity, privacy or compliance policies. Examples include unauthorized access to confidential data (like medical records or client files at a law firm) or improper management of data by employees (such as transporting data on a USB drive). An incident may not require official reporting to the governing regulatory authority. Incidents can vary in severity, but generally don’t materially damage the affected business.
- Some incidents become data **breaches** in which the exposure of non-public information meets a specific legal definition, as defined by an industry regulator (such as HIPAA for healthcare, or PCI for credit card transactions), privacy legislation (like the California Consumer Protection Act) or state breach legislation.

While it’s impossible to predict the specific harm caused by any particular future incident, it is still possible to make informed strategic and operational decisions about managing cyber risk.

Common Misconceptions

Cybersecurity and corporate governance are complex domains and it should come as no surprise that misconceptions exist when the two intersect.

For an SMB's board of directors to fulfill their cybersecurity governance duties, it's important that all parties share a common understanding of the relationship between cybersecurity and corporate governance.

To that end, here are five of the most common and significant misconceptions which must be overcome to best enable a small or medium business to manage cyber risk.

Misconception: Cybersecurity is only an IT issue and shouldn't be part of corporate governance

Information technology has evolved faster than perhaps any other domain in human history. Where once "computer" referred to a human job, now the term almost lacks specific meaning as all manner of devices include embedded computational capabilities.

Desktop computers which kept workers tethered to a single location are becoming a relic of the past—an intermediate stage of the evolution of business between manual desk-based labor and the cloud-hosted, increasingly mobile, ever-more-interconnected reality of today.

In the early days of the Internet revolution, cybersecurity was largely limited to client-based antivirus and firewalls. Over time, intrusion detection and prevention devices appeared. Crude port- and signature-based solutions gave way to behavioral recognition powered by machine learning.

This IT-oriented past shaped the thinking of a whole generation of executives, but it is already dangerously outdated. When the environment around us changes, changing with it is the key to survival.

Thinking about cybersecurity as only an IT issue fails to recognize the degree to which modern business relies on information as its lifeblood. High-profile attacks have inflicted enormous damage upon businesses through direct financial loss, reputational harm, regulatory penalties, failed insurance claims, or other legal fallout. When IT systems are taken offline, the whole business grinds to a near-halt.[7]

Without downplaying or diminishing the impact of these attacks, one positive outcome is that they have promoted cybersecurity squarely into risk management discussions. Boards, advisors and investors are now recognizing that cybersecurity is a business imperative, and not simply an IT issue.[8]

[7] For instance, Travelex being held to ransom by hackers explains that "The company has resorted to carrying out transactions manually, providing foreign-exchange services over the counter in its branches."

[8] Harvard Law School Forum published Prioritizing Cybersecurity: Five Questions for Portfolio Company Boards

Misconception: Reporting should be high-level or simplified

Board members are intelligent people who are skilled at analysis and metrics-driven decision-making. Boards are well-versed with financial metrics but lack operational context when presented with cybersecurity metrics such as port-calling or mean-time-to-recovery (MTTR). For this reason, many security leaders oversimplify (or “dumb down”) cybersecurity reporting.

This approach is a mistake—with potentially dire consequences—because it prevents the board from considering all pertinent information when making crucial cybersecurity decisions.

A second reason why reporting becomes dangerously high level is due to the perception that board members are so busy that the information supplied to them needs to be compacted. Important details are obscured within averages and lower-probability (but still significant) risks are omitted from discussion. Once again, the result is that decisions are made with incomplete information.

Furthermore, information anemia or transparency can lead to squandering scarce resources on non-strategic spend, leading to inadequate sustainability planning and creating slow time to value.

Finally, a third motivation behind relying on high-level metrics is to deliberately obscure unpopular information. This lack of transparency is a clear mistake and opens up the organization to risks which could otherwise be managed.

When reporting, organizations should avoid jargon that needs translation. The presentation of the cyber risk information should be characterized and quantified in business terms. For example, rather than saying, “We need more security budget to improve our ability to detect malicious activity because we are experiencing more phishing attempts than last year,” consider instead, “Last month we were victims of <A> ransomware incidents that cost us <B> dollars in bitcoin ransoms and <C> days to return to normal operations. The daily cost of this disruption was <D> in terms of lost orders, delayed shipments, increased warehousing costs, productivity costs, salaries, etc.”

Board members have the capacity and, increasingly, the interest to learn about cybersecurity matters which impact the business. Instead of oversimplifying or distilling cybersecurity reports, a better approach is to help to educate the board members so that they understand the concepts and consequences, in general, while saving tactical and technical details for occasional deep-dive sessions.

Consider the recommendation of NACD or NCSC board obligations: boards require access to cybersecurity expertise. It’s about helping board members interpret meaningful data rather than presenting sterilized metrics that provide no value in the decision-making process.

Misconception: Board members are already receiving the information they need

Too many organizations have a misplaced satisfaction that the board is already receiving the information they need to fulfill their governance obligations.

Business priorities, cyberthreats and the organization's operational context change over time and sometimes suddenly. Metrics and information which were sufficient a few months ago might have dangerous blind spots today.

Plus, many risk management plans and business continuity plans (BCPs) fail to adequately consider third-party dependencies (e.g., supply chains and manage services) or the potential impact of long-tail ("Black Swan") events.[9] Similarly, incident response (IR) plans are often generic and don't specify courses of action in enough detail, contributing to uncertainty when circumstances require clear instructions.

To stay on top of cybersecurity and risk management, it's important to regularly challenge assumptions about what information the board needs and about the readiness of the organization to respond.

Misconception: Compliance implies security

Most businesses today have a well-developed understanding of the regulatory environment in which they operate and their degree of compliance. However, some make the mistake of assuming that compliance in one area (for example, PCI) is suggestive of competence in another (for example, cyber risk management).

Or—even worse—they assume that compliance is synonymous with security. A firm can be compliant within a standard like HIPAA, but at the same time be vulnerable to cyberattacks.

This confusion and conflation can lead to well-intentioned, but mistaken, reports to the board which suggest a stronger cybersecurity posture than is warranted.

Misconception: There is a single best approach to managing cyber risks

If only it were this simple. The reality is that there are countless risks, every organization—even SMBs—has unique exposure and risk tolerance and resources vary enormously by organization.

The board must help management to identify which risks should be avoided, which should be accepted, which should be mitigated and which should be transferred.

In most cases in general, but especially for SMBs, managing cyber risk involves leveraging a combination of internal resources and third-party solution providers, plus purchasing insurance.

[9] While the exact nature and timing of specific events is by definition unpredictable, it is nonetheless a certainty that *something* will happen *at some point*

Enabling Cybersecurity Program Governance

Enabling cybersecurity governance requires an effective governance structure, board visibility into the right metrics and an appreciation of the relative dynamism of security needs.

An effective governance structure

The most effective SMB governance structures come from a combination of top-down principles that define the objectives and operational approach of a complementary bottom-up effort.

From a bottom-up perspective, the information security organization (perhaps simply the IT department or even a single individual) needs to be able to recommend the type of structural reporting they believe is necessary.

Cybersecurity reporting typically flows through the IT director into the CIO, who has ultimate responsibility for the security elements of governance. Unfortunately, this structure can create conflicts of interest. Today, many enterprises are adopting structures in which cybersecurity reporting goes to the COO, CSO, or Chief Risk Officer. Of course, it's relatively rare for an SMB to have a dedicated Chief Strategy or Risk Officer, but most do have a COO.

A complementary approach is to supplement the organization with a virtual CISO who may bolster independent support while leaving the final risk decision to the COO.

At the same time, the board needs to recognize the flaws and trade-offs inherent within any reporting structure and consciously advocate for an approach which will provide them with the information and visibility they need.

Metrics that matter

In today's information-rich operating environments, producing data is straightforward; however, delivering what's needed to enable effective cybersecurity governance requires careful consideration.

Metrics have maximum value when they capture an operating reality and can be placed in context. When these conditions are met, metrics reveal how you are performing today and how your performance is changing over time in the operating context of your business and risk environment. These insights enable the board to make decisions which help the business get to (or remain in) a desired state.

Broadly, metrics can be divided into two categories:

- Lagging metrics look into the past and tell the board things like the number of incidents, the likelihood that an incident results in a breach, the time to containment, the costs incurred and the effectiveness of an organization's incident response capability; these metrics are relatively easy to produce, as they tend to be counting- and measurement-based, but it is important to normalize them to account for changing scales
- Leading metrics take a forward-looking approach and capture information like the threat surface, the organization's readiness to respond to an incident and how investments are going to be operationalized in pursuit of cybersecurity goals; these metrics are more challenging to produce and for that reason they are often overlooked or perpetually exist just beyond the to-do list

Both sets of metrics are valuable. Moreover, they are connected: for instance, an Incident Prevention score should have value as a predictor of an organization's Incident Response capability. Care should be taken to ensure leading metrics hold real meaning and aren't simply vanity scores with little predictive value.

As an example, Table 1 lists metrics which hold value for the board of a mid-sized healthcare facility.

Regulatory	Industry	Compliance	Operations	Incident Response
• HIPAA/OCR Settlement Trends • HIPAA/OCR Violations (number of records and types) • HIPAA/OCR Mock Response • New Regulatory Requirements (NYDFS, GDPR)	• Industry Threat Comparison • Institutional vs. Peer Threats • Marquee/High-Priority Threat Intelligence (NH-ISAC plus vendor)	• Open High-Priority Regulatory Audit Findings • Policy Violations (numbers and types) • Policy Near Misses (numbers and types) • Training Results (number complete and average score) • Friendly Attack Results (number of phished credentials and reports)	• Security Budget (percent of IT) • Cybersecurity Maturity Status/Progress • Open High-Priority Risk Audit Findings • Patching Cadence • Red-Blue Team Exercise Results	• Mean-time to Response • Downtime Caused by Incidents • Lost Revenue Caused by Incidents • Incidents Reported to Media (numbers and duration) • Incidents Affecting Public-facing Systems (numbers and duration)

Table 1 *Metrics should hold real meaning to provide predictive value and enable informed decisions*

Operating timeframes

When it comes to cybersecurity, all businesses—small, medium and large—must adjust their thinking regarding operating timeframes. Often, this thinking is shaped by annual planning cycles and long-term horizons, so it needs to be recalibrated to account for the dynamic nature of the risk environment in which the business operates. For instance, requests for funding should be considered very quickly, as they may be in response to a threat which has only just materialized.

Likewise, the organization must be able to execute with velocity: there's little point in quickly making the correct decision if teams don't have the resources to take action.

Knowledge Domains for Cybersecurity Program Governance

When it comes to understanding and governing an SMB's cybersecurity program, it's convenient to divide the broad subject into separate knowledge domains.[10]

Situational awareness

Situational awareness pertains to the company's present state with respect to cybersecurity and examines factors including critical business services, the role of IT operations, identified cybersecurity risks, known attacks, compliance obligations and the status of penetration testing programs and other cybersecurity initiatives.

Strategy and operations

While situational awareness is largely about the present, strategy and operations takes a higher-level approach. It relates to a company's capabilities and the frameworks (e.g., NIST, ISO, etc.) and processes which determine those capabilities.

Understanding strategy and operations also includes understanding a company's partners and service providers, insurance decisions, employee training programs and approaches to dealing with employee mobility.

Insider threats

Because external attackers garner most of the attention, insider threats are all-too-frequently overlooked. Nevertheless, they pose significant risk owing to their levels of access and the trust given to them.

Combating the risk associated with insider threats requires understanding operational controls (including encryption, back-ups, network monitoring, etc.), hiring policies, cross-functional cooperation (for instance between HR and IT), written policies and the specific actions needed to respond to an insider incident.

[10] To help boards develop and maintain their understanding, the National Association of Corporate Directors (NACD) offers an excellent resource, Questions for the Board to Ask Management about Cybersecurity

Incident response capabilities

Incident response is a crucial component of corporate governance. Incidents—whether attacks or not—can compromise personal and business data, severely impact operations and even lead to legal consequences, so it's imperative to respond quickly and effectively when they occur.

Organizing an effective IR capability requires making major decisions and carefully prescribing a large collection of actions. The company must decide what services are needed to respond to an incident, which team structures are most appropriate and where necessary expertise can be found and secured—potentially including external parties.

Plus, the nature of cyber incidents can be broad, so response should recognize and address cross-departmental roles and responsibilities based on the incident classification (e.g., event, incident, breach).

Supply chain and third-party risks

The 2019 Spiceworks report on third-party risk exposed that half of the 650 respondents had experienced a material breach as the result of a vendor. What's worse, only 15 percent of those breaches were reported by the victimized vendor.

Taking stock of supply chain and third-party risks requires applying—as much as is possible—all the other knowledge domains to these external parties. In practice, this means asking them the same questions which are asked internally.

This domain can be subdivided into two others: the risks facing a company's supply chain and third parties (and their capacity to manage those risks), and the procedures and mechanisms which govern how a company interfaces with those external parties.

Conclusions and Recommendations

Cybersecurity governance is a team communication and risk management activity. Transparency is essential: information sender and information receiver must be on the same page for effective governance.

Simple steps to improve transparency and coordination include examining the current state of cybersecurity governance structure, reviewing the relevance of metrics and the effectiveness of their reporting and presentation, plus committing to making ongoing updates to the company's risk register. Diving into more detail, here are 10 recommendations companies can follow to improve cybersecurity governance:

1. Have the board or senior management team evaluate trusted third parties to provide an independent assessment of the company's cybersecurity governance and cybersecurity program domains. As needed, modify structure to obtain better alignment, transparency, and oversight of knowledge domains.
2. Endeavor to express cyber risk appetite in a quantifiable way to guide the use of available resources.
3. If not already established, identify important data, information assets and systems critical to achieving the objectives of the business.
4. Have a trusted third party technically assess whether security configurations and other technical and process controls adequately protect the critical data, assets, and systems.
5. Quantify current cybersecurity spending in terms of dedicated full-time employees, security technologies, and imputed cross-departmental processes.
6. Reconcile the assessment of the governance structure, program domains and spending; evaluate irreconcilable gaps as improvement opportunities to create an improvement roadmap.
7. Consider third-party resources and solutions providers to augment capabilities that are not core or not cost-effectively sustainable.
8. Recognize tools without strong competencies and sustainable processes are likely already, or will soon become, shelf-ware.
9. Identify all relevant cybersecurity metrics. Note those that are shared with the board and determine if they are useful leading or lagging metrics. Enlist trusted third parties to provide independent guidance on establishing sustainable metrics reporting.
10. Survey your board for reporting improvements; Suggest reporting improvements to the board.

About eSentire:

eSentire, Inc., the global leader in **Managed Detection and Response (MDR)**, keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $6 trillion AUM, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit **www.esentire.com** and follow **@eSentire**.

About UHY Consulting:

UHY Consulting, Inc. provides consulting services that inspire, transform, and achieve the unimaginable. Through our national team of consultants, we serve clients worldwide from the Fortune 1000 to the dynamic middle market. Our mission is to solve and transform our clients' evolving business challenges embracing a philosophy we call 'The Next Level of Service.' We help our clients prosper and our employees to realize their potential through our four strategic priorities: client centricity, innovation, market development, and our people development. We offer consulting services in four areas: Transformation Solutions; Software Solutions; Resource Solutions; and Technology, Risk & Compliance.