OPTIV

RISKY BUSINESS:

Solving Cyber Insecurity with a Risk-Centric Business Model.

WHITE PAPER

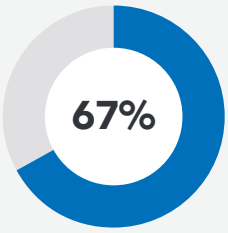
Introduction

Traditional compliance assessments are similar to taking a picture with an old Polaroid™ instant film camera. Historically, risk managers would complete an annual assessment and, like the point and click of a camera, the assessment would take a picture of what the risk landscape looked like in a specific moment in time. The business could check the box, annual assessment complete.

The problem? That picture does not capture the activity occurring the other 31,535,999 seconds of the year. This lack of knowledge of the fluctuating activity within an enterprise environment, or cyber insecurity, is detrimental in today's digital economy. The rapid adoption of digital technologies and IoT, coupled with an increasingly sophisticated and active threat landscape and constrained resources, demand businesses remain vigilant every second, every day of the year.

Many businesses are confusing security with compliance and maintaining a check-the-box, compliance-based approach to cybersecurity. As security initiatives continue to move to the forefront within organizations, security teams are also challenged to translate IT speak into business terms. In fact, 67% of boards of directors are putting pressure on senior executives to increase management involvement in risk oversight.[1] Articulating overall security health to the business and board in a real-time and business-friendly manner is more important now than ever.

It's time for a risk revolution. Businesses must fundamentally rewrite how to manage cybersecurity to achieve business resilience. Optiv Security recommends cybersecurity professionals change the narrative. Security risk can no longer be confined to a conversation about IT; rather it must be integrated into the fabric of business strategy. And, while it's true that today's growing digital technologies, Internet of Things (IoT), regulations and a challenging threat landscape have made the jobs of risk management teams more difficult, it is absolutely possible to solve cyber insecurity with a risk-centric business and IT integration approach.



of boards of directors are putting pressure on senior executives to increase management involvement in risk oversight.

This paper explores the evolution of risk management and why security teams are becoming a critical component of the overall business risk strategy, and considers how:

- The introduction of digital technologies, including cloud and IoT devices, changes the landscape of traditional cybersecurity risk.
- Mitigating this increased risk requires a transition in approach and program from prevention tactics, to proactive and intentional risk decision-making by understanding threats, vulnerabilities and countermeasures.
- Rapidly changing infrastructure, strategy and data usage requires security teams to be agile enough to support new business initiatives.
- Knowing and articulating overall security health is critical in today's increasingly competitive digital economy.
- The separation of business risk and security risk can no longer occur. Risk management must be integrated throughout the business.

This paper also describes how businesses can transform cyber insecurity into a risk-centric business program that is not only compliant, but both balanced and grounded in thoughtful risk management.

RISK = THREAT x VULNERABILITY x IMPACT

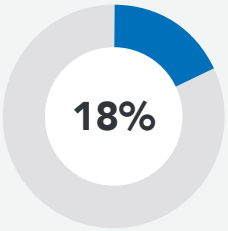
A Risk Recap

Risk is not a new business phenomenon. Every industry carries its own inherent risk. The hospitality industry regularly navigates labor risk, an employee walk-out could result in financially devasting consequences. Manufacturing businesses face operational risk or potential loss from failed internal processes, people or systems. The financial services industry is significantly impacted by financial risk related to how much debt a business carries, loss of revenue, exchange and interest rates, etc. And, no industry manages risk more regularly than healthcare. Here, concerns over data privacy and compliance pale in comparison to that of patient risk. Risk management in this industry is truly a matter of life or death.

While most businesses can talk to the fundamental risks they manage, they may not align consistently on their definitions of risk across the business. For example, cybersecurity historically did not speak in the same risk language as other parts of business because business risk is commonly managed separately, outside of the purview of IT and cybersecurity teams. Optiv sees this frequently. In 2018, company research shows that 22% of organizations assessed scored a medium rating or higher for their overall security strategy, and only 18% scored high in the aligning of the business objectives with their security program management.[2] Security teams need to design business-aligned risk management programs to be effective.

The separation of risk management from other areas of business risk can no longer occur. Risk transformation is about enabling the business to make healthy business-based decisions on where to accept and where to mitigate risk. To successfully do this, risk professionals must identify and understand enterprise risk holistically in order to become consistent in how risk appetite is determined and acted upon.

Risk professionals refer to risk appetite as the amount of risk an organization is willing to take on while achieving their business objectives. Determining risk appetite is a key step in evaluating risk posture. Is a business risk adverse, or risk tolerant? More and more often businesses tend to be risk tolerant and able to operate in risky business situations. Still, other organizations are more risk averse and manage that against policies and controls in the environment to create the right security and risk model for its specific business. A company's risk posture is largely determined by the industry it operates in, and the size of the business. Financial service organizations are typically risk averse when it comes to information risk. This is largely because financial data equals transactions, which can equate directly to actual currency or financial loss. These organizations typically have a more mature risk management program than a manufacturing organization that manages different types of risk.



of organizations in 2018 scored high in the aligning of business objectives with their security program management.

Many security teams:

1. Know what they are doing, or not doing, in their security program, but do not have a good handle on how that applies to the overall risk posture of the business.
2. Have a good understanding of their threat landscape and what threat actors are up to, but are so focused on the threat that they are missing the business impact.
3. Are not business-outcome focused when they are trying to communicate risk to their executives or boards.
4. Do not continuously monitor risk or pay attention to incidents as they occur.

It's time for businesses to transform traditional risk management programs to integrated risk management strategies. The process of risk management needs to involve the entire business. Many security practioners get caught up in IT and security and forget the whole purpose of security is to enable a system so that the business can use it to make money. If security practioners do not work with the business to identify goals, and business leaders do not view security risk as a part of the overall risk posture, the business cannot spend appropriately on the security required to protect desired business outcomes.

Risk transformation *is about enabling the business to make healthy business-based decisions on where to accept and where to mitigate risk.*

The Digitization of Business

Security is reported to be the number one challenge area *for organizations executing on digital transformations.*

While risk management is not a business phenomenon, digital transformation (DX) – or the evolution and transformation of business models through digital technologies – certainly is. The digital workplace has impacted every aspect of risk as we know it. In fact, 86% of survey respondents agree or strongly agree that the digital world is creating new types and levels of risk for their business.[3] Security teams are challenged to keep up as change seems to be the only constant. Many industries, such as retail and hospitality, whose main risk priority used to be protecting credit card data are now focused on data privacy in a broader sense. The rapid adoption of digital technologies to enable business introduces complex security challenges, yet security budgets and resources remain the same. Digital transformations and IoT require a whole new level of IT. Security teams need to recognize that part of effective risk management is taking what exists today and utilizing continuous risk monitoring to enable rapid adaption to a changing threat landscape.

Traditional risk management approaches air gapped control networks to isolate them. In fact, historically some systems were not built with security in mind because they were never meant to connect to the Internet, or even other computers. Take the evolution of the automotive industry, for example. Years ago, cars were manufactured with an indicator light that would turn on to notify the owner to make an appointment to take it in for service. Today, cars are self-reporting maintenance data back to manufacturers and dealers who then call owners to coordinate service appointments. Not only does the automotive industry have to account for operational risk in building the cars, the introduction of IoT now requires the management and protection of an influx of new data and a plan to mitigate the physical risk involved with self-driving cars. In the event a self-driving car injures a pedestrian, it is a physical risk – and also an IT problem.

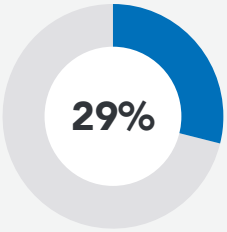
Conventional risk policies and assessment regimens are no match for today's increasing volume and velocity of change. The rapid adoption of third-party platforms and technologies adds additional complexity in protecting proprietary data that is collected and stored outside of the business perimeter. Data issues came in as the third most challenging area for organizations executing on DX at 23%; security was reported as the most challenging with 31% followed by technology strategy at 26%.[4] Optiv research validates this challenge with data classification, data loss prevention/leakage and cloud data security ranking as the top three challenges reported.[5]

Not only does DX introduce a massive amount of new data to manage and protect, it vastly expands the enterprise attack surface – introducing additional risk. Gartner reports that 77% of survey respondents think investment in risk management and risk management practices are not keeping up with new and higher levels of risk arising in a more digital world, creating greater exposure for their business/entity.[6] Many businesses do not take inventory of what their enterprise attack surface is comprised of, and do not have the capability to protect it. This is largely because they lack the context needed to do so. The why, who and where; this context provides the ability for security teams to move faster because they do not have to pause and ask where the data is – instead they can immediately manage the countermeasures put in place to protect it. This lack of context is likely why it takes 191 days to identify the average data breach.[7]

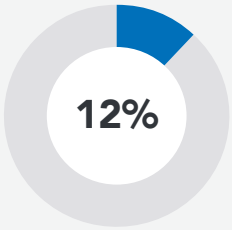
From January 1, 2017 to March 20, 2018, 1,946,181,599 records containing personal and other sensitive data were compromised.[8] Yet, 77% of respondents in a recent survey of 2,800 IT professionals say their organizations do not have a formal cybersecurity incident response plan in place.[9] These statistics demonstrate how widespread a problem data security has become. Optiv has found data classification, data loss prevention/leakage and cloud data security are the top three 2018 client challenges. The fact is many organizations do not have a mechanism to locate all of their data, yet alone secure it. And when the data is unsecured, it's up for grabs. The Optiv Attack and Penetration teams gained access to client systems – and in many cases data – through weak or default passwords in 40% of Q2 2018 client engagements.

This may be the direct result of many organizations considering check-the-box compliance a security program. Compliance does not enable adaptive, risk-based decision making. In fact, only 29% of companies maintain compliance a year after validation. This means that many businesses are simply checking boxes or adding compensating controls, and then forgetting about it until the next audit is due.[10] In other words, businesses can no longer assess risk on an annual or semi-annual basis and assume the findings from that compliance assessment activity – or snapshot of a moment in time – are still valid and provide enough protection to secure an enterprise's digital footprint.

Imagine if the hospitality industry only assessed risk to food quality on an annual basis? Or, a petroleum refinery only assessed equipment risk once a year. If you examine how a business monitors its other risks you will find it is much more frequent, often in real-time, which is vastly different than how many organizations assess and measure cybersecurity risk. Organizations can no longer afford to take a Polaroid™ picture of their security environment once a year and expect to protect it. The digitization of the business demands all industries monitor cybersecurity risk in the same fashion as other business risks – in a proactive, ongoing and real-time manner.



of companies maintain compliance a year after validation.



of organizations assessed scored a medium rating or higher for the ability to report solid security metrics.

Articulating Risk to the C-Suite and the Board

Communicating overall security health to the C-suite and board has long been a challenge for cybersecurity teams. Only 12% of organizations assessed scored a medium rating or higher for the ability to report solid security metrics.[11] Why? Typically these groups speak different languages. Security teams are well versed in speaking to the number and types of threats they are protecting the business from, which compliance regulations they have met or are preparing answers to, reporting the results of vulnerability scans or providing the number of patches recently completed. However, the board does not care about bits and bytes, or identity and security-specific language. What they care about is risk, financial loss, availability and downtime. In order to have an intelligent conversation with business leaders, security professionals have to translate this IT speak into how these issues impact overall business objectives.

These groups have a hard time communicating because they are not working from the same dictionary. Security teams commonly classify risk in categories of low, medium and high. Business leaders often do not know or share these definitions as their priorities are often far different than that of the security teams. To effectively communicate with one another, and to successfully manage collective business risk, these two teams must find common ground and work together to define risk terminology so they can work from the same playbook.

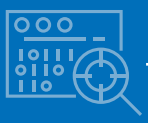
Interpretive guidance from organizations such as the National Association of Corporate Directors (NACD) and the Securities and Exchange Commission (SEC) is available to help security teams translate IT speak into business impact. However, this is not prescriptive, it is simply guidance. Cybersecurity risk and its potential for loss and damage increases every day, so it is getting more and more scrutinized by executive leadership teams. Security teams need to communicate to the board exactly what they want to know:

1. What are the critical assets?
2. Who would try to get them?
3. What is in place to stop them?
4. Where are there gaps?
5. What measures are in place to detect and respond should they get past preventative controls?
6. What is the financial impact to the organization in case of an incident?

The fact is, when it comes to risk management enterprises cannot do it all. They need to decide what they should do based on their specific business.

NACD GUIDANCE

What the Board Wants to Know:[12]



Did cyberattacks occur and how severe were they?

What are the company's cybersecurity risks, and how is the company managing these risks?

How will we know if we have been hacked or breached, and what makes us certain we will find out?

Who are our likely adversaries?

In management's opinion, what is the most serious vulnerability related to cybersecurity (including within our IT systems, personnel, or processes)?

If an adversary wanted to inflict the most damage on our company, how would they go about it?

Has the company assessed the insider threat?

When was the last time we conducted a penetration test or an independent external assessment of our cyber defenses? What were the key findings, and how are we addressing them? What is our maturity level?

Does our external auditor indicate we have cybersecurity-related deficiencies in the company's internal controls over financial reporting? If so, what are they, and what are we doing to remedy these deficiencies?

Activating on Standards to Build a Formal and Programmatic Process

Several independent agencies across many verticals provide repeatable risk mitigation standards. The Factor Analysis of Information Risk (FAIR), The International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), The International Federation of Consulting Engineers (FIDIC), Transportation Security Administration (TSA), United States Government, Securities and Exchange Commission (SEC) and many more have all provided ways businesses can keep track of controls in information security programs. In addition, guidance is provided by regulatory bodies, including The Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes Oxley Act of 2002 (SOX), the Payment Card Industry Data Security Standard (PCI DSS), the General Data Protection Regulation (GDPR), the North American Electric Reliability Corporation Critical Infrastructure Protection Plan (NERC CIP) and more. At Optiv, the PCI DSS is the most commonly framework utilized by clients, although it is truly not a framework at all.

The downside to all of this direction is that these risk frameworks and guidelines provide a notion that in order for risk management programs to be effective, businesses have to be compliant with all of the controls in these frameworks. There are 114 controls in ISO 27002, and NIST 800-53 can have up to 170 controls. It typically is not practical for any IT security program to be mature in all of these different controls.[13]

Optiv believes that organizations should leverage input from holistic, risk-appetite considerations to choose a baseline set of controls, a number of additional controls to be moderately mature in, and decide whether or not they need to implement some controls at all. Clients often select a control framework, start at the beginning of the framework and work all the way through to the end. There is an innate problem with this. ISO 27002 has 14 control domains; the last control domain is incident response (IR) management.[14] If businesses wait until they are highly mature in the rest of an information security program to employ an incident management program, it's too late. Incident management is a critical part of a security program that needs to be in place to proactively manage an incident when it occurs. Preparing for IR is typically one of the more cost-effective security measures an organization can take because well-planned IR reduces incident impacts and costs, and because security incidents are inevitable.[15]

If businesses wait until they are highly mature in the rest of an information security program to employ an incident management program, it's too late.

MATURITY MODEL OVERVIEW

Where does your organization need to be?

Aware
Foundational awareness, at a tactical level, with a focus on plannning and strategy development

Reactive
Focus on tactical, ad-hoc approach to program components where identified deficiencies are addressed as-needed leveraging technology

Adaptive
Shift away from reactive to strategic operation, with a focus on program development through formalization of evidence-backed requirements and objects

Purposeful
Development of security mechanisms and business-aligned guidance formally integrated into plan, build and run cycles

Strategic
Focus on proactive capabilities to anticipate business need and provide innovative solutions, and drive innovation

This is where the frameworks fall short. An effective risk management program does not need to check every box. Most businesses that strive to be highly mature in the totality of these frameworks will often be unsuccessful. The industry a business is in, and how mature their risk program already is, will determine what framework to follow. Frameworks are a guide from which to measure gaps. Businesses need to ensure they have the basics covered by choosing a handful of immediate controls that are needed to protect from breach, put the right people in place and decide how to move closer to compliance by choosing the right controls for their specific business. Risk management is not a prescriptive exercise. It is an ongoing process that aligns controls to unique business drivers and industry specific threats and then continuously adjusts based on benchmarks, fluctuating business priorities, compliance mandates and real-time risk monitoring.

Risk management = *Undertaking a privacy and governance process to determine where to focus efforts on cyber resilience and risk optimization and monitoring.*

Businesses must go beyond meeting annual guidance to build and enforce a continual risk management process. A holistic approach to define risk from the inside out, and outside in, enables security teams to build a unique risk policy to meet exacting business requirements. This approach requires visibility into their entire risk profile. However, 65% of organizations indicate they have recently experienced an operational surprise due to a risk they did not adequately anticipate.[16] Annual risk assessments are not enough in today's rapidly evolving digital landscape. Successfully managing risk requires a 360 degree view to define risk tolerance and weight budget to tolerance – what are businesses willing to risk vs. invest in?

Risk Management Best Practices Vary by Industry

Security teams find it difficult to keep up with change. Evolving risk, compliance, business and IT landscapes create new exposures. And the increasingly large and puzzling security product landscape makes it a major challenge to pick an effective and cost-efficient mix of controls.[17]

All businesses carry risk and must make tough decisions based on tolerance vs. investment. The type of business determines what is important. Organizations that write their own applications care about application security and attack surface management far more than third-party risk. If a business outsources all of that, third-party risk management would rank far more important. The point being, every business is different and needs to manage its risk in a different way.

Security and risk management teams need to facilitate risk conversations instead of setting mandates. A conversation enables leaders to come to agreement on the likelihood of an incident occurring, what an incident might cost and what countermeasures can be put in place. With the global average cost of a security breach now at $3.86 million, or $148 per data record, this conversation is critical.[18]

Conducting a business outcome risk conversation is a completely different conversation than a compliance conversation, and one that would unite and benefit business and security leaders alike.

Optiv believes that businesses focused on building cyber resilience would benefit from strengthening:

- Cybersecurity program development
- Risk management
- Enterprise incident management
- Threat management, detection and response

At least half of all organizations surveyed admit they face skills gaps in three key areas: threat prevention (56%), threat detection (50%) and threat analysis (50%).[19]

Businesses looking to optimize risk management and monitoring should consider:

- Continuous risk monitoring

Two-thirds of organizations say their in-house cybersecurity capabilities are adequate to protect against cyberthreats, yet nearly 80% say they have been breached within the past year.[20]

- Third-party risk management

$3.86 M

the global average cost of a security breach.

Don't Live in Fear of the Next Cyber Threat

It's time to change the risk conversation. IT risk management needs to transform to integrated risk management where security is a fundamental component of overall business risk strategy. Businesses can solve cyber insecurity with a proactive and continuous risk management strategy. It is not possible for businesses to achieve high maturity in every control – and it is futile to try. Instead, businesses need to pursue the right level of maturity for controls based on holistic and consistent consideration of risk appetite.

IT risk management needs to transform to integrated risk management where security is a fundamental component of overall business risk strategy.

Weaving cybersecurity throughout a business strategy enables an enterprise to:

- Continuously monitor and manage risk
- Identify and close security gaps
- Maintain compliance
- Adapt and scale to meet shifting business priorities
- Clearly articulate and improve overall business heath
- Influence better decision-making, faster

Take the Next Steps

Optiv believes cybersecurity leaders should work collaboratively with business leaders to:

1. Define risk appetite and management terms.
2. Align security program management to business objectives.
3. Pursue the right level of maturity for controls based on unique business needs.
4. Identify what the board wants to know and how best to communicate that information.
5. Keep communication lines open to continually monitor, manage and communicate overall security health.

Authors

Dustin Owens, Vice President/General Manager, Risk Management and Transformation

Brian Golumbeck, Executive Director, Risk Management and Transformation

Gregory Thompson, Executive Director, Risk Management and Transformation

Robert Santiago, Practice Manager, Risk Management and Transformation

Contributors

Megan Ruszkowski, Corporate Writer

References

1. AICPA, The State of Risk Oversight, 2017.
2. Optiv, 2018.
3. Gartner Market Insight: 10 Business Outcomes Every IRM Solution Must Deliver, August 2018, figure 1.
4. Forrester, Fix Your Culture Gaps to Speed Up Digital Transformation, February 2018.
5. Optiv, 2018.
6. Gartner Market Insight: 10 Business Outcomes Every IRM Solution Must Deliver, August 2018, figure 1.
7. Ponemon Institute, Cost of a Data Breach Study, 2017.
8. Privacy Rights Clearinghouse, 2018.
9. Ponemon Institute, The Third Annual Study on the Cyber Resilient Organization, Sponsored by IBM Resilient, 2018.
10. Verizon's PCI DSS Compliance report, 2015.
11. Optiv, 2018.
12. NACD Cyber-Risk Oversight Handbook, Management Questions, 2017.
13. Optiv, Blog Series: Frameworks in Context, 2018.
14. Optiv, Blog Series: Frameworks in Context, 2018.
15. Gartner 2019 Planning Guide for Security and Risk Management Published 5 October 2018.
16. AICPA, 2018 The State of Risk Oversight in conjunction with the American Institute of CPAs.
17. Gartner 2019 Planning Guide for Security and Risk Management Published 5 October 2018.
18. 2018 Cost of a Data Breach Study, sponsored by IBM, Ponemon Institute.
19. AT&T Global State of Cybersecurity survey, 2017.
20. AT&T Global State of Cybersecurity survey, 2017.

Want to learn more?

Visit go.optiv.com/risky

Optiv Global Headquarters
1144 15th Street, Suite 2900
Denver, CO 80202
800.574.0896
www.optiv.com

3.19 | F1.1