OPTIV

SHARE:

THE TRUTHS AND MYTHS ABOUT CYBERSECURITY RISK

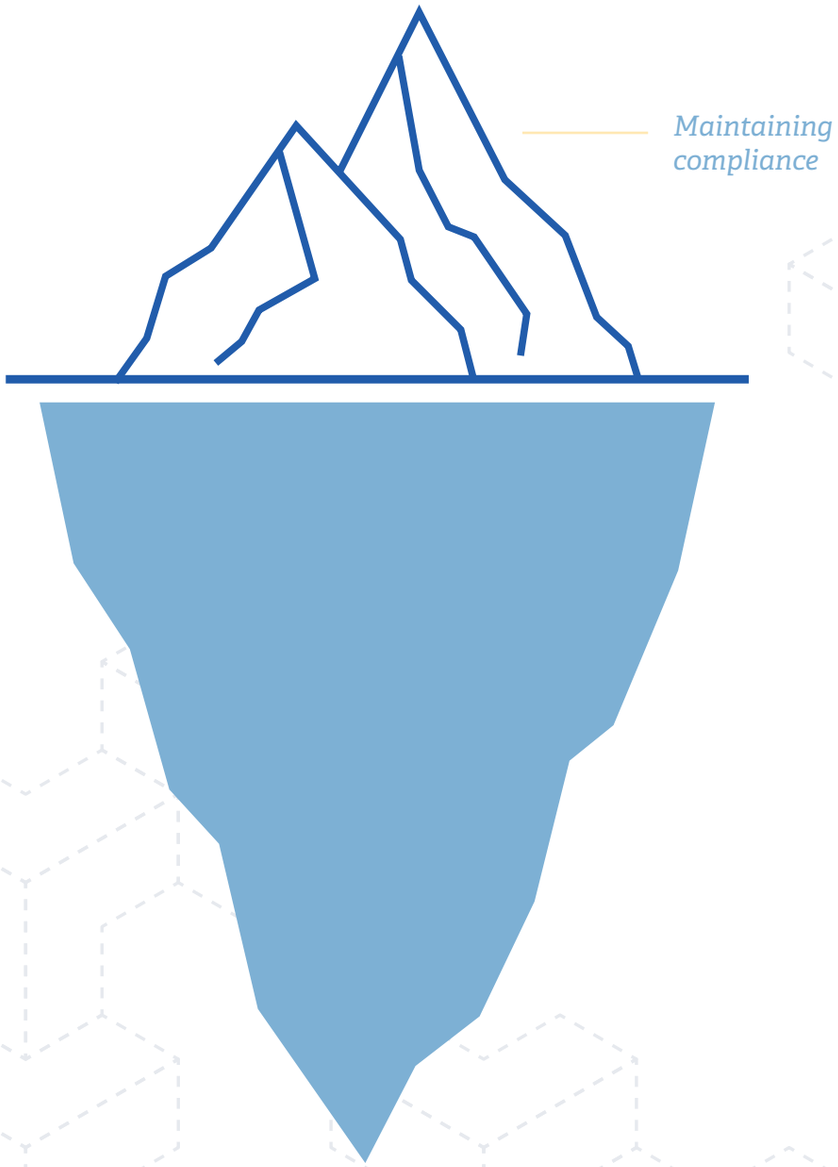
The digital and security landscape is constantly evolving, as are cybersecurity threats and priorities.

Today's organizations need to adapt to a growing volume and velocity of change by shifting their approach from reactionary box-checking to a proactive risk-centric security strategy. This requires a fresh risk perspective that aligns security strategies with business objectives to reduce operational risk. Understanding the truths and myths surrounding cybersecurity can help you begin to align your security needs around the business goals of your organization.

MYTH

If you're in compliance, you're secure.

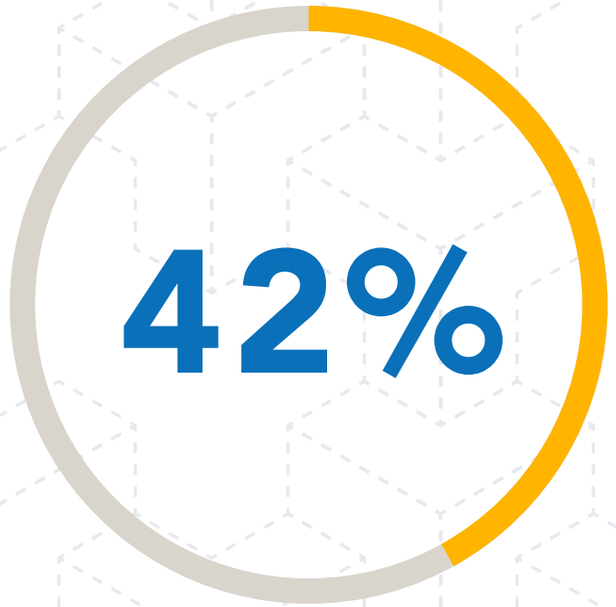
Your organization is highly complex and so are the risks you face. Imagine maintaining compliance as the tip of the iceberg when evaluating risk, it's the bare minimum and compliance does not always equal security. The time has come to think beyond tools and frameworks and focus on securing your entire digital landscape. In doing so, compliance becomes an outcome of an effective, comprehensive security program.



MYTH

Managing third-party risk is not necessary.

A growing dependence on vendors and partners to conduct business has resulted in third-party risk becoming a great concern. In a recent survey, 42% of respondents said their goal is to improve controls over third parties' access to their sensitive and confidential data.[1] Businesses must manage this risk, and ensure partners follow appropriate standards, to avoid additional exposure. As organizations face issues associated with reputation, profitability and regulations, it's critical to establish a process to streamline and simplify third-party risk management as part of an overall risk management strategy.



of respondents said their goal is to improve controls over third parties' access to their sensitive and confidential data

TRUTH

Manual processes are roadblocks to reducing vulnerabilities.

Security teams are inundated with alerts from multiple sources, making it challenging to keep pace with the ever-changing cyber threat landscape. It's not uncommon for organizations to rely on an assortment of spreadsheets to track assets and vulnerabilities, relying on staff to identify and resolve issues by hand. Ponemon notes that more than half of their survey respondents (51%) say their security teams spend more time navigating manual processes than responding to vulnerabilities, leading to insurmountable response backlogs. Additionally, almost half of respondents (48%) say their organizations are at a disadvantage in responding to vulnerabilities due to the use of manual processes.[1]

TRUTH

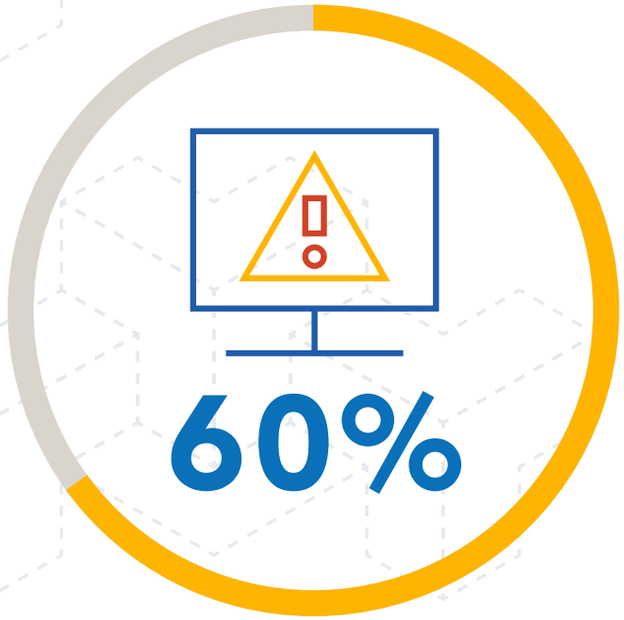
A new approach to understand overall risk is needed.

Security organizations can no longer operate in a silo; they need to partner with the business to effectively and holistically manage cybersecurity risk with business risk. Taking this new approach can help organizations transition from preventative risk management to proactive and programmatic risk management. This modern strategy leverages proactive incident detection and response capabilities coupled with continual threat analysis, to reduce overall risk and improve the ability to communicate comprehensive business health.

MYTH

Businesses are not attacked more than once in 24 months.

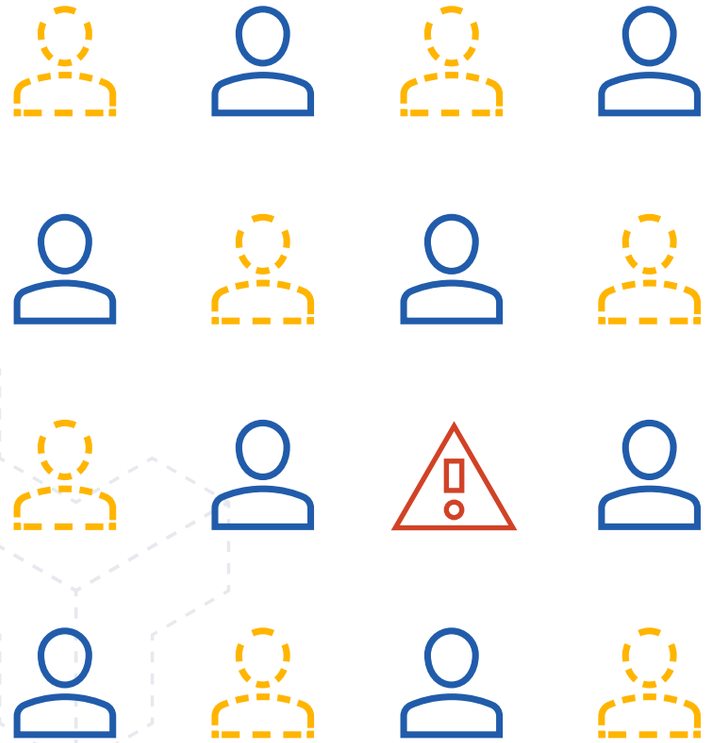
Cyber attacks are relentless and continuous with malicious threat actors constantly probing for new vulnerabilities as the business changes on a daily basis. In fact, a recent Ponemon survey reveals 91% of the participating organizations had experienced at least one damaging cyber attack over the past two years. And, 60% indicated having two or more incidents resulting in a combination of data breaches, significant disruption and downtime to business operations.[1]



indicated having two or more incidents resulting in a combination of data breaches, significant disruption and downtime to business operations

TRUTH

Cybersecurity staffing shortages may be putting your organization at risk.



As skilled security staff becomes scarce and budgets remain tight, organizations are struggling to grow their security programs, maintain workloads and maximize technology investments. Without trained staff, how can your organization address challenges such as staying current on necessary security regulations, adapting infrastructure to meet changing business needs or expertly implementing and managing new technologies? Choosing the right partner enables you to improve detection and response capabilities, reduce risk and increase operational uptime.

At Optiv, we solve operational risk challenges by weaving cybersecurity into the fabric of organizations.

Learn How

1 Ponemon, Measuring & Managing the Cyber Risks to Business Operations, December, 2018.

Optiv Global Headquarters
1144 15th St, Suite 2900
Denver, CO 80202

800.574.0896 | optiv.com

Optiv is a market-leading provider of end-to-end cybersecurity solutions. We help clients plan, build and run successful cybersecurity programs that achieve business objectives through our depth and breadth of cybersecurity offerings, extensive capabilities and proven expertise in cybersecurity strategy, managed security services, incident response, risk and compliance, security consulting, training and support, integration and architecture services, and security technology. Optiv maintains premium partnerships with more than 350 of the leading security technology manufacturers. For more information, visit www.optiv.com or follow us at www.twitter.com/optiv, www.facebook.com/optivinc and www.linkedin.com/company/optiv-inc.

2.19 | F1