Creating trust in the digital world

EY's Global Information Security Survey 2015

EY
Building a better working world

EY's Global Information Security Survey investigates the most important cybersecurity issues facing businesses today. It captures the responses of 1,755 participants around the globe and across sectors, and our findings and conclusions are based on those insights and on our extensive global experience working with clients to help improve their cybersecurity.

The following findings show that organizations are making progress in improving the way they respond to today's cyber threats and attacks, but they also indicate there is a need for considerable improvement as the world becomes more digital and attackers increase their sophistication and persistence.

Operating in a digital world invites new challenges and threats

- Smart devices and services can deliver unintended consequences and amass vulnerable data.
- Social media is "always on" and information widely shared, without a full appreciation of privacy and security.
- Information is increasingly stored in the cloud or with third parties, resulting in less control, increased risk and a more complex cyber ecosystem.
- Human behaviors are changing in positive and negative ways.
- New legislation and regulations are forcing changes in processes that can open up new vulnerabilities and widen the attack surface of the organization.

Is your cybersecurity ready to support your digital business?

- Do you understand the specific threats and vulnerabilities in your digital world?
- Have you done the work and thinking required to determine how that threat landscape applies to your organization and strategy?
- Do you know how to set your risk appetite, to determine the acceptable and unacceptable loss and harm from potential incidents, and to prioritize cybersecurity measures around this?

Only when the risk appetite is set at a level that the board is comfortable with, and that the organization can achieve, will your digital transformations be sustainable.

Key findings

88%
of respondents do not believe their information security fully meets the organization's needs

59%
see criminal syndicates as the most likely source of an attack today

42%
of respondents say that knowing all their assets is a key information security challenge

67%
of respondents do not see managing the growth in access points to their organization as an information security challenge in the Internet of Things (IoT)

47%
of respondents do not have a Security Operations Center (SOC)

57%
of respondents say that lack of skilled resources is challenging information security's contribution and value to the organization

54%
of organizations do not have a role or department in their information security function that is focusing on emerging technology and its impact

49%
say an increase in funding of up to 25% is needed to protect the organization in line with management's risk tolerance

36%
say it is unlikely they would be able to detect a sophisticated attack

36%
of respondents do not have a threat intelligence program

How can you increase the chances of stopping an attack?

Organizations are familiar with good risk management principles, and the same can apply to cybersecurity:

Key risk management principles ...	... applied to cyber risk
1 **Focus on what matters most** Must align to your unique business and risk culture	**Know your critical information assets** Identify critical business assets most vulnerable to cyber attack
2 **Measure and report** Include qualitative statements and quantitative measures	**Make cyber risk more tangible** Clearly define cyber risk and underlying metrics
3 **Comprehensive in nature** Should cover all risk types, current and forward-looking	**Align with existing risk frameworks** Financial, operational, regulatory, customer, reputation, etc.
4 **Allocation of risk appetite** Allocation of appetite to business units and risk types	**Make cyber risk relevant to the business** Link organizational-level risks to individual business units and their information assets
5 **Integrate with business planning** Regulators are increasingly looking for evidence	**Embed risk appetite in investment decisions** Prioritize investment where critical, empower businesses to make informed local decisions

Cybersecurity is a digital enabler

Cybersecurity is not an inhibitor in the digital world; rather, it is a way to help make the digital world operational and sustainable. Cybersecurity is key to helping unlock innovation and expansion, and a tailored organization and risk-centric approach to cybersecurity can adjust the balance of the digital world back toward sustainability and safety, to better protect your organization and create trust in your brand.

The shift to Active Defense

Understanding your critical cyber business risks and knowing what attackers may want from your organization helps enable you to establish "targeted defense," and assessing the threat landscape allows you to understand the most likely threat actors and methods they may use. This all informs your SOC and should be the basis on which it will support your organization.

Putting in place a more advanced SOC and using Cyber Threat Intelligence to align operations helps enable Active Defense which involves: sending out intelligent feelers to look for potential attackers, analyzing and assessing the threat, and neutralizing the threat before it can damage your organization's critical assets.

Is Active Defense appropriate for your organization?

If any of these statements applies to your business, you should consider an Active Defense approach:

- We have a SOC, but are still not finding evidence of advanced attackers.
- We have a SOC, but we still had a major breach.
- We have an outsourced SOC, but our intellectual property and business systems are not truly secure.

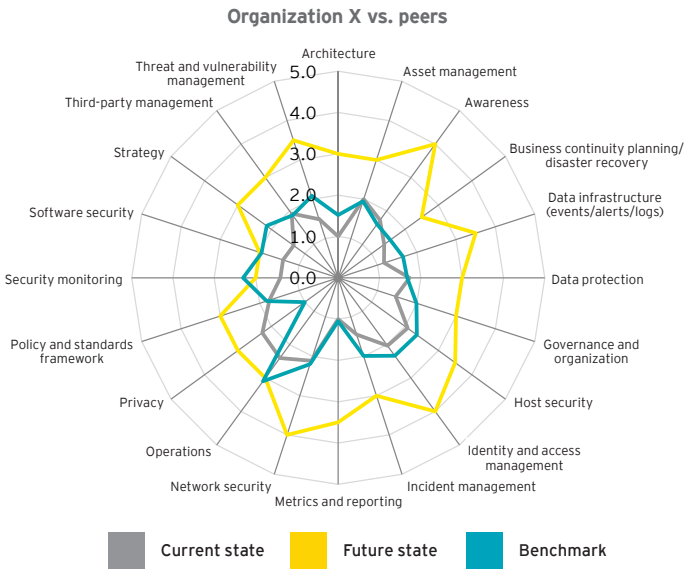
The road to improvement

Any organization can benefit from an objective assessment of its information security programs and structures that assists with:

- Understanding your organization's risk exposure
- Assessing the maturity of your current cybersecurity program and identifying areas for improvement
- Building a prioritized road map for project investments and organizational change initiatives
- Collecting information to create benchmarks against other organizations
- Determining whether your security investments have improved your security posture

This assessment needs to be broad and high-level, as well as totally immersive in specific areas and components. Dashboard metrics enable an organization to see what is needed to support the ongoing assessment, transformation and sustainability of the information security strategy.

An example of current state maturity benchmarking



EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no.AU3608
ED None.