Path to cyber resilience: Sense, resist, react

EY's 19th Global Information Security Survey 2016-17

EY
Building a better working world

Global findings

EY's Global Information Security Survey investigates the most important cybersecurity issues facing organizations today. It captures the responses of 1,735 participants around the globe from over 20 industry sectors. We base our findings and conclusions on those insights and our extensive global experience of working with clients to help them improve their cybersecurity programs.

The following findings show that organizations are making progress in the way they sense and resist today's cyber attacks and threats. But, the results also indicate the need for considerable improvement if organizations want to stay operational while the world becomes more connected, and attacks become more devastating.

The state of cyber resilience

The threat landscape changes and presents new challenges every day. Over decades, organizations have learned to defend themselves and respond better to potentially catastrophic events. Repeated financial crises, geopolitical shocks, terrorist attacks and the explosion in cybercrime have all driven organizations to evolve their approach to being resilient.

Cyber resilience is a subset of business resilience; it is focused on how resilient an organization is to cyber threats. The components of cyber resilience are:

Sense

Sense is the ability of organizations to predict and detect cyber threats and attacks.

Resist

Resist mechanisms are basically the corporate shield. It looks at how much risk an organization is prepared to take across its ecosystem, and then establishes the three lines of defense.

React

This is the readiness of the organization to deal with the disruption, through incident response capabilities, crisis management and then forensic investigation. This is also how the organization is brought back to business as usual and adapted, and to improve cyber resilience tomorrow.

Download the report at ey.com/giss.

Key findings

86%

say that their cybersecurity function did not fully meet their organization's needs.

57%

of organizations rated business continuity management their joint top priority, alongside data leakage and data loss prevention.

57%

of responders have had a recent significant cybersecurity incident.

42%

do not have an agreed communications strategy or plan in place in the event of a significant attack.

86%

of responders say they need up to 50% more budget.

64%

do not have, or only have an informal, threat intelligence program.

89%

of organizations do not evaluate the financial impact of every significant breach.

62%

would not increase their cybersecurity spending after experiencing a breach which did not appear to do any harm.

The overall picture

	Sense (see the threats coming)	Resist (the corporate shield)	React (recover from disruption)
Where do organizations place their priorities?	Medium	High	Low
Where do organizations make their investments?	Medium	High	Low
Board and C-level engagement	Low	High	Low
Quality of executive or boardroom reporting	Low	Medium	Low

Today's emergency services: the cyber breach response program

Given the likelihood of suffering a cyber breach, organizations must develop a strong, centralized response framework as part of their overall enterprise risk management strategy.

A centralized, cyber breach response program (CBRP) is the focal point that brings together the wide variety of stakeholders that must collaborate to resolve a breach, and is able to manage the day-to-day operational and tactical response, plus be equipped with in-depth legal and compliance experience, as these events can trigger complex legal and regulatory issues with financial statement impact.

The CBRP goes beyond the capacity of a traditional program management office. It can help ensure that:

- An organization's business continuity plan is appropriately implemented
- A communication and briefing plan among all internal stakeholders is developed and enforced
- All breach-related inquiries received from external and internal groups are centrally managed

In addition, it oversees the process of evidence identification, collection and preservation, forensic data analysis, and impact assessment, and can also direct and modify the investigation on the basis of fact pattern.

A robust CBRP, therefore, enables a cost-effective response that mitigates breach impacts by integrating the stakeholders and their knowledge, and helps the organization navigate the complexities of working with outside legal counsel, regulators and law enforcement agencies.

Key characteristics of a cyber-resilient enterprise

Understands the business
Cyber resilience demands a "whole-of-organization" response – an in-depth understanding of the business and operational landscape.

Understands the cyber ecosystem
Map and assess the relationships the organization has across the cyber ecosystem, identify what risks exist and perform a risk assessment.

Determines the critical assets – the crown jewels
Most organizations overprotect some assets and under-protect others. In the survey, only 11% rated patented 'intellectual property (IP) the number one or number two most valuable information type.

Determines the risk factors
Over and above all of the technologies and tools that can provide better intelligence and identification of threats, is collaboration. Sharing information about the risk and threat landscape allows the organization to understand their broader risk landscape and expose any security gaps.

Manages the human element with exceptional leadership
After a cyberattack, and with technology supporting the entire organization, every employee will be impacted. Clear communication, direction and example setting from leadership will be essential, as well as clearly defined roles or tasks that will help the organization become operational again.

Creates a culture of change readiness
Organizations that develop superior, integrated and automated response capabilities can activate nonroutine leadership, crisis management and coordination of enterprise-wide resources. Simulation exercises and war games can challenge the existing crisis management, command and control center, manuals and plans.

Conducts formal investigations and prepares for prosecution
The CIO and CISO together with executives from security, general counsel, external counsel, investigations and compliance, can collect evidence. Together, they can establish whether the attackers still have footholds in the organization and whether harmful malware or ransomware could sabotage the organization again. They can also investigate who carried out the attack, and how, and be able to bring a claim against the attackers.

If you would like to find out more about EY's cybersecurity, contact:

Andreas Toggwyler	+41 58 289 59 62	andreas.toggwyler@ch.ey.com
Tom Schmidt	+41 58 289 64 77	tom.schmidt@ch.ey.com

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. 00645-173GBL

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com/giss