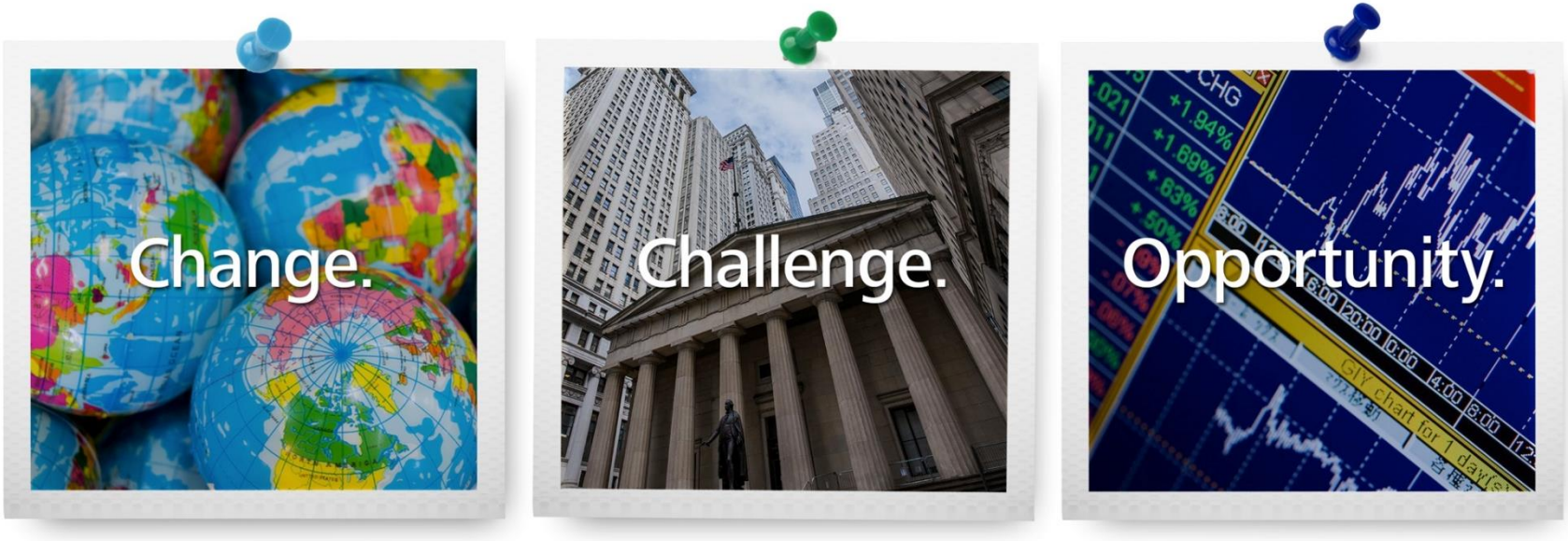
Deloitte.

powered by The CFO Program



CFO VISION 2015

November 11–13 | Washington, D.C.

CFO Lens
Relevant, CFO-centric content

Deloitte.

powered by The CFO Program

CRISIS

Building cyber resiliency: Tools, techniques, and metrics that matter

Emily Mossburg, Principal, Deloitte & Touche LLP

Rick Siebenaler, Principal, Deloitte & Touche LLP

Deloitte.
CFO Lens
Relevant, CFO-centric content

Agenda

- The innovations that drive growth also create cyber risk
- Cyber resilience is a moving target
- A systematic approach to achieving and sustaining cyber resilience
- Top actions and questions for finance executives

The innovations that drive growth also create cyber risk

Threat actors exploit weaknesses that are byproducts of business growth and innovation.

- M&A or corporate restructuring
- New customer service and sales models
- New sourcing and supply-chain models
- New applications and mobility tools
- Use of new technologies for efficiency gains and cost reduction

Perfect security is not feasible. Instead, reduce the impact of cyber incidents by becoming:

SECURE —
Enabling business innovation by protecting critical assets against known and emerging threats across the ecosystem

VIGILANT —
Gaining detective visibility and preemptive threat insight to detect both known and unknown adversarial activity

RESILIENT —
Strengthening your ability to recover when incidents occur

Cyber risk management is a positive aspect of managing business performance.

Cyber resilience is a moving target

Cyber resilience is the capacity to sustain critical business operations in the event of a cyber incident while reducing damage to assets and supporting an accelerated recovery to normal operations.

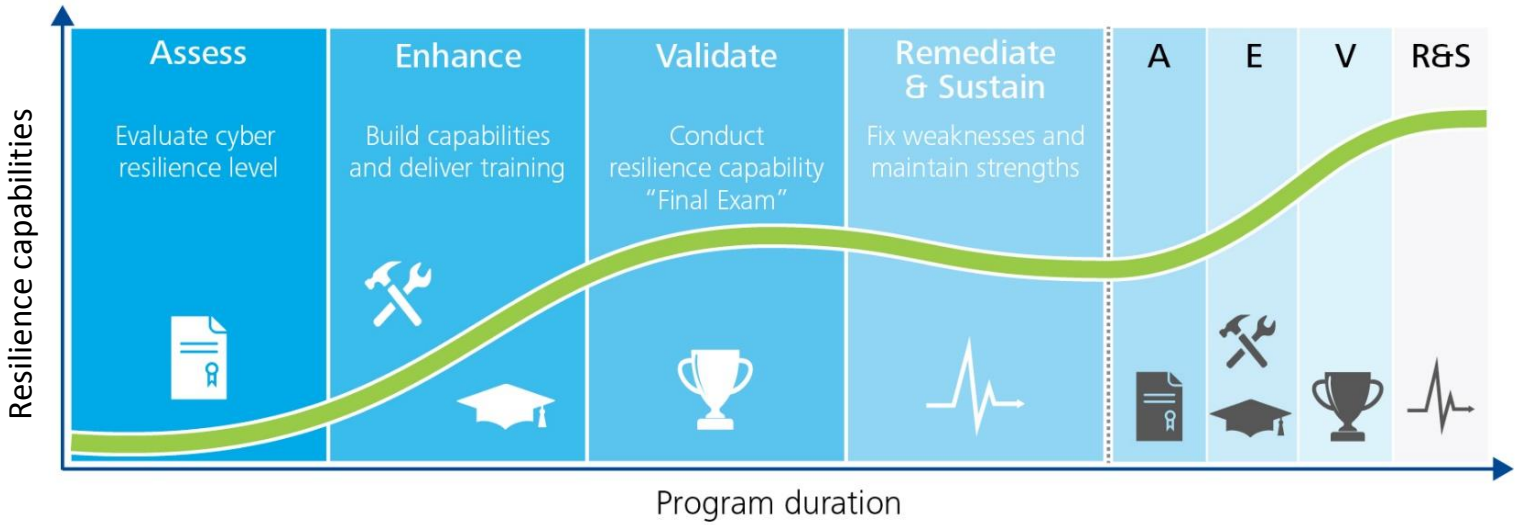
Maintaining cyber resilience is a challenge for many organizations because of:

The fast pace of business	The evolving cyber threat landscape
▪ New lines of business and business operating models ▪ Technology and business process enhancements and upgrades ▪ Personnel, regulatory, and third-party changes	▪ Increasing frequency, sophistication, and volume of cyber attacks ▪ Emerging cyber vulnerabilities and a disappearing cyber perimeter ▪ Expansion of the impact of cyber events, incidents, and outages

Combined with the tendency for skills and readiness to erode over time, the fast pace of business and the evolving cyber threat landscape make maintaining cyber resilience a moving target.

A systematic approach to achieving and sustaining cyber resilience

Organizations should achieve and sustain their targeted cyber resilience posture by leveraging an ongoing regimen of resilience capability assessment, enhancement, validation, and remediation/sustainment activities.



Recommendations for success

Leverage a "crawl – walk – run" model to enhance capabilities

- For organizations with a basic level of cyber resilience, enhancement efforts should focus on developing core resilience capabilities.
- For organizations with an advanced level of cyber resilience, enhancement efforts should focus on integrating and embedding cyber resilience into day-to-day operations.

Prioritize efforts based upon organizational objectives and risk

- Organizations should prioritize efforts to enhance capabilities that mitigate the greatest amount of risk and/or align with organizational objectives to the greatest degree — for many organizations, this means focusing on basic "blocking and tackling" vs. the latest and flashiest risk being discussed in the industry or marketplace.

Don't quit while ahead

- To maintain a targeted level of cyber resilience, organizations should continue to invest — cyber resilience is not a "once and done" capability.
- It is easier to maintain than build — an ongoing regimen of activities supporting cyber resilience should drive the highest return on invested resources.

Top actions and questions for finance executives

Actions you need to own

- **Put a senior executive at the helm.**
  He or she must be able to lead in a crisis and also guide the program and enlist collaboration across diverse functions.
- **Map threats to business assets and understand potential business impacts.**
  Set direction, purpose, and risk appetite for the program. Establish priorities and provide funding and resourcing.
- **Drive early wins.**
  Establish momentum by focusing on pilot initiatives that have a measurable impact on business success. Use these to plant the seeds of long-term cultural change.
- **Accelerate behavior change.**
  Create active learning scenarios that instill awareness of the impact of daily activity on cyber risk. Embed cyber risk management goals into the evaluation key executives.
- **Trust but verify.**
  Conduct monthly or quarterly reviews of key risks and risk metrics, and then address roadblocks.

Questions you need to ask

- **Are we focused on the right things?**
  Understand where innovation is driven and how to embed a culture of cyber risk awareness within the innovation life cycle.
- **Do we have the right talent?**
  Quality over quantity. There is not enough talent to do everything in-house, so take a strategic approach to sourcing decisions.
- **Are we proactive or reactive?**
  Retrofitting for security is very expensive. Build it upfront in your management processes, applications, and infrastructure.
- **Are we incentivizing openness and collaboration?**
  Build strong relationships with partners, law enforcement, regulators, and vendors. Foster internal cooperation across groups and functions, and ensure that people aren't hiding risks to protect themselves.
- **Are we adapting to change?**
  Policy reviews, assessments, and rehearsals of crisis response processes must be regularized to establish a culture of perpetual adaptation to the threat and risk landscape.

About Deloitte's CFO Program
The CFO Program brings together a multidisciplinary team of Deloitte leaders and subject matter specialists to help CFOs stay ahead in the face of growing challenges and demands. The Program harnesses our organization's broad capabilities to deliver forward thinking and fresh insights for every stage of a CFO's career – helping CFOs manage the complexities of their roles, tackle their company's most compelling challenges, and adapt to strategic shifts in the market.