



Government & Higher Education **5x5** Cyber Change series:
A five-minute read to inspire new ways of thinking about cybersecurity

Unlocking new risk insights



Cyber risk can come from anywhere: a malicious email; a compromised chip; a hacked vendor. Today, organizations face an era of "cyber everywhere" as hyper-connectivity combines with a myriad of Internet of Things (IoT) devices and other emerging technologies to expand attack surfaces. Organizations have the ability to respond to this significant growth in cyber risk through advances in artificial intelligence (AI) and modeling techniques for identifying and quantifying cyber risk. According to Deloitte's 2019 Future of Cyber Survey¹, only half of the C-level executives who responded use any form of quantitative risk-evaluation tools (including financial loss models). Quantifying risk can help prioritize the cyber approaches you take and better direct you to manage your most impactful risks with the ultimate goal of protecting and enhancing citizen's trust. Are you ready to measure your cyber risk?

5 insights you should know

The true cost of a cyberattack is often beneath the surface. Spanning from loss of intellectual property, damage to public trust, and damages to national security or the economy (including operational disruption).²

No one is immune. In our 2019 Future of Cyber survey, 90% of respondents admitted to a disclosure of sensitive data from their test environments in the past year. Digital transformation will continue to play a role in expanding risks.

New vulnerabilities are emerging. COVID-19 has expedited the digitization of workforces and the growth of online access to services, challenging traditional security protocols.

It's difficult to see the full risk picture. Cyber scorecard tools are helpful, but only tell part of the story, failing to communicate risks in dollar and mission terms.

Standing still is dangerous. Aging legacy systems can be a key source of risk. Quantifying that risk can help prioritize which systems need modernization first.



5 actions you can take

Assess your risk. Consider implementing a data-driven cyber risk quantification (CRQ) methodology to demonstrate, in financial terms, the cost of cyber risks.

Make sure you have the right data. Effective quantification frameworks should consider both external and internal data to help enrich, inform, and calibrate the quantification model.

Visualize the risk and connect the decisions. Create dynamic views of decisions relevant to the lens of affected stakeholders.

Put the right talent in place. Focus on upskilling existing staff to understand and perform CRG.

Develop a repeatable CRQ capability. To keep pace with burgeoning cyber threats and help prioritize spending, organizations should consider implementing repeatable modeling processes to allocate funding efficiently.

Connect with us

Tim Li

Principal
Government & Public Services
(GPS) Cyber & Strategic Risk Lead
Deloitte & Touche LLP
timli@deloitte.com

Kelly Miller Smith

Principal
GPS Cyber
Deloitte & Touche LLP
kellysmith@deloitte.com

John Gelinne

Managing Director
GPS Cyber
Deloitte & Touche LLP
jgelinne@deloitte.com