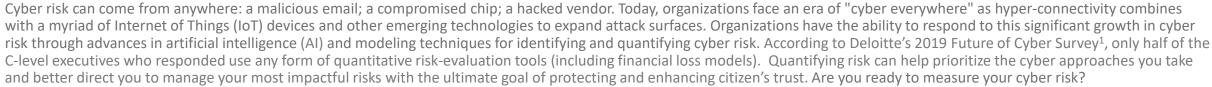
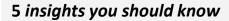
# Deloitte.

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

## Unlocking new risk insights





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).<sup>2</sup>

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

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. Deloitte shall not be responsible for any loss sustained by any person who relies on this publication

1:. Deloitte, 2019 Future of Cyber Survey, March 2019 2.3: Deloitte, Quantifying cyber risk to chart a more