2023 CSMFO ANNUAL CONFERENCE

BACK TO THE CAPITAL

SACRAMENTO

JANUARY 31 - FEBRUARY 3, 2023

Board/Council Cyber Risk Management

What your City Council Needs to Know about Cyber Risk

CSMFO California Society of Municipal Finance Officers

Speakers

Donald E. Hester

City of Livermore

Cybersecurity Manager

DEHester@LivermoreCA.gov

Twitter @sobca

Ron Puccinelli

City of Menifee

Chief Information Officer

RPuccinelli@CityofMenifee.us

Local Government Officials Guide to Cybersecurity

- Preface
- Why the guide
- Executive Summary
  - 3-6 pages
- 5 Key Principles
  - 3 pages each
- Conclusion and Summary
  - 1 page
- Appendix (toolbox)
  - As needed

- Local Government Officials Guide to Cybersecurity (LGOGC) Workgroup
- Writers
- Reviewers
- Researchers
- Project Manager

ICMA LG Cybersecurity Survey 2020

Local Governments at Risk

- Top officials in organizations are often not engaged in cybersecurity at high levels
- Top management is not sufficiently well informed about or committed to cybersecurity
- Top officials fail to insist on a cyber safe culture
- Top officials fail to act appropriately in their own cyber responsibilities

“ It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts.”

President Obama, White House, May 29, 2009

"…each city and town council should hold public discussions, at least annually, on their cybersecurity measures, which would also raise awareness among residents and local organizations on ways to improve cybersecurity."

"78.6% responded that their governments provided mandatory cybersecurity training annually to the mayor/elected county executive, city/county council members, department heads, and average end-users."

- ICMA LG Cybersecurity Survey 2020

- Cyberattacks: A Growing Threat to Marin Government - Marin County Civil Grand Jury - May 11, 2020

Cyber Risk

- Everyone is touched by the digital world (entire ecosystem)
- Rapid move to digital government
- Increased reliance on technology
- Increased digital (cyber) risk
- Cyber risk is enterprise risk
- Impact on all government operations
- The impact can be devastating or debilitating to operations
- There is a need for cyber resiliency for local governments
- Understanding the responsibility for Council/Board

Cybersecurity is a Top Risk

- Municipal governments face many of the same risks as private sector businesses including cyber risks
- Global Risk Report, World Economic Forum
- American Water Work Association
- AICPA
- CISA, Department of Homeland Security
- CalCPA
- PwC, 2022 Global Risk Survey

One of the most important **stakeholders** responsible for managing cyber-risk is the board of directors.

California Society of CPAs May 2020

Cyber Risk

- Growing cyber threats and a greater reliance on data in business models mean that cybersecurity is now a central responsibility for the entire C-suite and board.
- An even bigger signal of the growing concern around cyber is that 51% of board members cited it as a serious risk (and another 35% as a moderate risk) — more than any other category of business leader.
- First, virtually all companies are now digital companies, with a heavy reliance on data and analytics and a growing reliance on mobile and cloud.
- Second, cyber threats continue to grow and become more sophisticated.

Cyber risk is not an IT issue

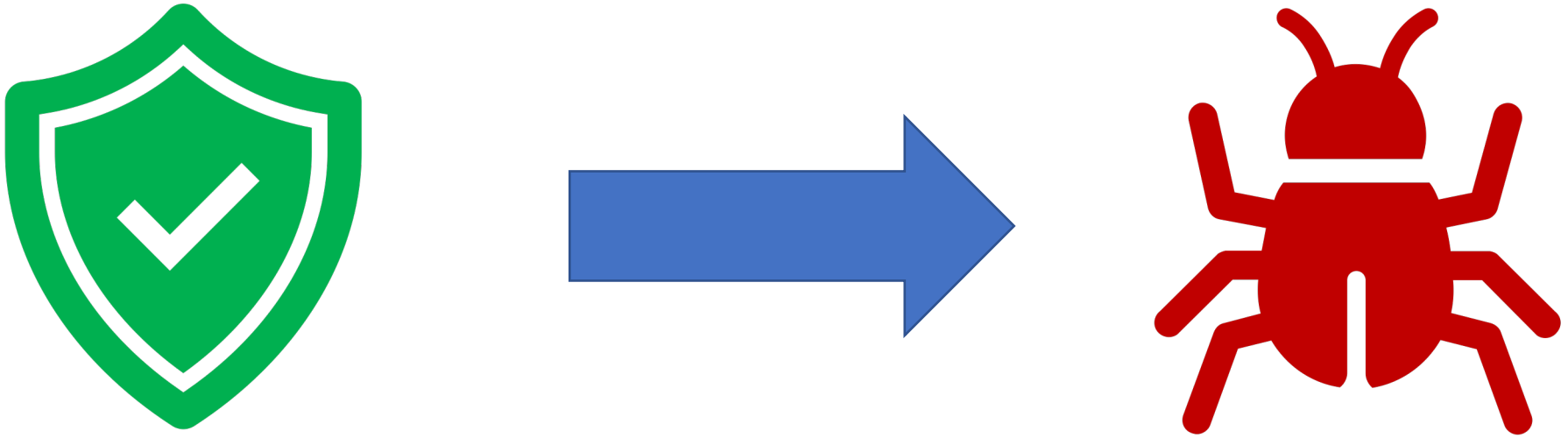
What services does your LG deliver?

Cyber risks impacts all of them

Cybersecurity is not an IT issue.

Cybersecurity is our response to cyber risk.

Not all cyber risks are related to IT.



Cybersecurity is your organization’s response to Cyber Risks

Some Cyber Risks outside of IT

- Operational Technology
- Disinformation
- Privacy
- Ethical Use of Technology especially AI
- Compliance
- Critical Infrastructure
- Convergence of Information and Physical Security

ICMA LG Cybersecurity Survey 2020

Cyber risk is critical for Local Governments to understand, especially top elected or appointed officials

- The cyberthreats their government faces
- Actions they should take to protect information assets
- The gap between actual cybersecurity practices and what is needed to address those cyber risks
- The barriers that their government has in implementing cybersecurity

"Understanding these issues will enable local officials not only to see why cybersecurity is crucial to their government's digital well-being, but will help ensure that cybersecurity has their full support and is adequately funded and properly managed."

https://icma.org/articles/pm-magazine/look-local-government-cybersecurity-2020

ICMA LG Cybersecurity Survey 2020

Barriers to Cybersecurity

- Inability to pay competitive salaries
- Insufficient staff
- Lack of funds
- Lack of adequate training

(*all related to funding)

"Until local governments affirmatively address these and perhaps other barriers–especially funding, staffing, awareness, and support–they cannot expect to improve their cybersecurity outcomes or more effectively protect their information assets."

Risk management capabilities provide the greatest value to board members and business leaders when they are embedded within the organisation's strategic planning and decision-making processes.

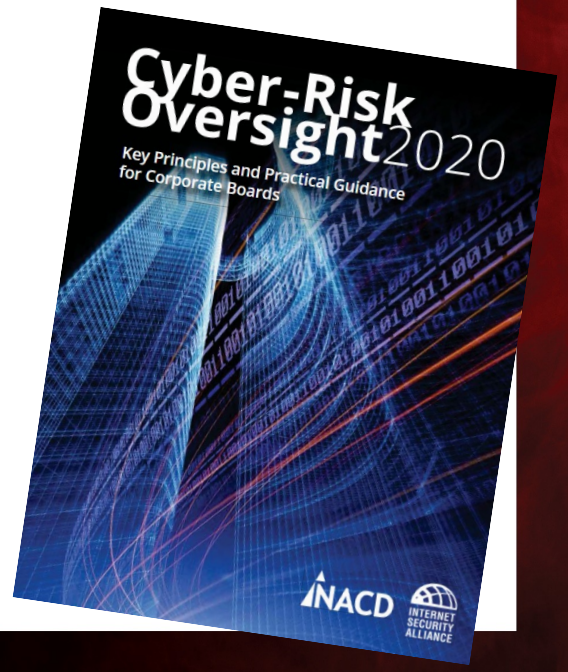
PwC 2022 Global Risk Survey

Many executives and boards still have dated views about cybersecurity:

"Board members need to ensure that management is fully engaged in making the organization's systems as resilient as economically feasible. This includes developing defense and response plans that are capable of addressing sophisticated attack methods."

Governance Roles for Boards/Councils

How should Council (board) view cyber risk?
What role does Council (board) play in managing cyber risks?
What expectations should Council (board) set for management?
What questions should the Council (board) be asking?



Key Principles

For elected and appointed local government officials

Understand cyber risk is enterprise risk and cybersecurity is strategic

Ensure budget is sufficient to reduce cyber risk to an acceptable level

Culture, Cyber Literacy, Clear Expectations, Accountability

Select a framework and assign responsibility for cybersecurity

Data and reporting sufficient for decision making

Enterprise Risk

Enterprise Risk

Understand cyber risk is enterprise risk and cybersecurity is strategic

- **Cybersecurity is the organizations response to Cyber Risk**
- **Cyber risk is not an IT problem, it is an enterprise problem**
- **Technology is not support, it is strategic and critical**
- **Cybersecurity has a cross-functional nature**
- **Cybersecurity is an integral element in a digital age**
- **Continuous evaluation of critical assets and risks**
- **Watch for the introduction of new risks**
- **Strike a balance between innovation and risk**

- **Council should have expectation that management will establish enterprise-wide cyber-risk management**
- **Legal, regulatory, compliance, and contractual risk**
- **Complex and constantly evolving**
- **High profile attacks can spawn lawsuits**
- **Reputation risks (loss of public trust)**
- **Reasonable oversight & neglect of fiduciary duty**
- **Council (board) participate in a cyber-breach simulation table-top exercise**
- **Transparent without revealing sensitive information**

Assign Budget

Assign Budget

Ensure budget is sufficient to reduce cyber risk to an acceptable level

- Barriers to cybersecurity are all related to budget
- Assigning budget to cybersecurity demonstrates commitment to addressing cyber risks
- Difficult to separate all expenses in IT
- Organizations put some cybersecurity expenses in different line items – no true apple to apples comparison
- Determining whether the spending is justified and defensible in light of public scrutiny

- Industry average 15% of IT budget
- Local Government lower than industry benchmarks
- GFOA average 3% of IT budget
- NASCIO 0-3% of IT budget
- ICMA Survey 0-10% of IT budget

Oversight

Oversight

Culture, Cyber Literacy, Clear Expectations, Accountability

- As cyber threats grow responsibility and expectations grow
- Similar to financial literacy, Council needs cyber literacy
- Cybersecurity is an essential element of many board-level decisions
- Education needs to regularly refreshed will grow quickly stale
- Set clear expectations with management
- Inherent bias on the part of management to downplay true state of risk

- Virtually all decisions before the Council have an impact on cyber risk
- Spend time with the security team outside the board room
- How does CISO collaborate with the other departments
- Understand the CISO role and mandate
- Full Council briefing at least quarterly or as situation warrants
- Council should have access to cybersecurity expertise – start with expertise within the org
- No one size fits all will apply everywhere

Framework

Select a framework and assign responsibility for cybersecurity

Framework

- Evaluate barriers to cybersecurity
- Legacy reporting structures
- Legacy decision making processes
- Siloed operating models (doing their own thing)
- Not fully taking into account interdependencies of modern systems
- Select a framework and adapt it to your needs
- Council should see that management has an enterprise-wide approach to cybersecurity

- ISA-ANSI Integrated Approach to Managing Cyber Risk
- Ownership of cyber risk is cross-departmental not CIO (IT)
  - Assign to CISO, CRO, BISO etc… (Enterprise Risk)
- Team cross-department with all stakeholders
- Forward looking risk assessment
- Include compliance requirements
- Collaborative approach
- Separate budget from IT

Monitor & Report

Data and reporting sufficient for decision making

Monitor & Report

- Perfect cybersecurity is an unrealistic goal
- Managing risk is continuous not a goal
- Cyber has grown to become strategic
- We have limited funds and need to balance risk
- Financial exposure to cyber risk is important to know
- Need to understand the economics of cybersecurity
- Cybersecurity will necessarily become a core component of overall government financial management
- Management should seek out the best data possible to make informed decisions
- Consult in-house or external experts
- Focus on the probable and high expected loss
- Calculate worse case, best case, and the most likely case scenarios
- Sufficiently resilient
- Economics in favor of the attackers
- The bad guys only have to get it right once, we have to get it right every time

Guidelines for Reporting

Metrics need to be:

- Be relevant
- Reader friendly
- Convey meaning
- Highlight change
- Show performance
- Concise
- Enable discussion and dialogue

Own the Problem

"These executives must appreciate, or learn, if need be, the true role that technology plays in the modern organization, including the financial risks that technology places on the organization and the steps that must be taken to manage risk appropriately."

- *The Financial Management of Cyber Risk (ANSI/ISA)*

Cyber risk does not belong to IT or Cybersecurity it belongs to the Council/Board