Paint a Picture of a Cyber-Resilient Organisation

The constant drip of cyber incidents has moved cybersecurity squarely into the C-Suite and Boardroom. Various security technologies can improve your risk posture, but technology alone is not enough. Cyber resiliency requires an ecosystem of efforts in three crucial areas: governance and policy, process and education, and technology and services.

IT leaders play a crucial dual role: oversee effective efforts and ensure a clear understanding among non-IT leaders.

Governance and Policy

ACTIONS FOR **IT LEADERS**

C-Suite/Board Engagement

Hold one-on-one conversations with leaders using real-world scenarios to show the business implications of possible events.

Dashboards

Summarise the complicated landscape in an intuitive and actionable way.

Governance

Ensure individuals impacted by a security decision have a chance to be heard.

Standards

Leverage a security standard as your guide, recognising that full adherence is moving target.

Strategy

Evolve your strategy to counter increasingly advanced attacks and match your organisation's culture.

Staffing

Grow talent within your department and lighten workloads by leveraging appropriate vendors and technologies.

Digital Trading Partners

Develop a thoughtful intake process to assess and remediate security risks; regularly audit and confirm necessity of third-party network access.

LESSONS FOR **NON-IT LEADERS**

C-Suite/Board Engagement

Security is a team sport—be sure to understand and establish your role.

Dashboards

Effective dashboards are actionable and indicate where to direct resources and attention.

Governance

Security and risk are essential considerations for all activities; include them as part of deliberations.

Standards

Standards evolve over time to meet ever-changing threats and require regular attention to keep up.

Strategy

Strategy must balance security ambitions with the operational needs of clinical and business workflows.

Staffing

Talented security staff is hard to find—a team approach to security encourages retention.

Digital Trading Partners

Third parties (vendors, partners, and affiliates) broaden your security risk—assess the security risks of any relationship.

Process and Education

Training

Provide continuous training; tune exercises to various roles and use a variety of communication channels.

Testing

Validate that staff apply their security training through campaigns using the latest scammer techniques.

Incident Response Planning

Get organised before an event: leverage predetermined templates and checklists, and pre-vet potential vendors.

Risk Assessments

Incorporate incremental risk assessments when a system changes or a new system is brought online.

Audits

Align internal audit, security, and IT to be able to share results, coordinate efforts, and potentially help each other with funding.

BCP[1] + Backups + DR[2]

Test DR, backups, and BCPs to ensure they work well together across all shifts of employees. Ensure leadership understands your RTOs[3] and RPOs[4].

Training

C-suite executives will be targeted due to their position and access to data—establish regular awareness training for executives.

Testing

They may feel sneaky, but internal phishing campaigns protect the organisation.

Incident Response Planning

The security team should be empowered with the authority needed to respond quickly to incidents.

Risk Assessments

Risk assessments can inform your security investment decisions and identify areas to get the most "bang for your buck."

Audits

External auditors look for evidence that you take security seriously.

BCP + Backups + DR

While temporarily inconvenient, practiced downtime makes unexpected down time easier and protects patient safety.

Technology and Services

Cyber Intelligence

Leverage cyber intelligence that is relevant, actionable, and tailored to your organisation.

Cyber Insurance

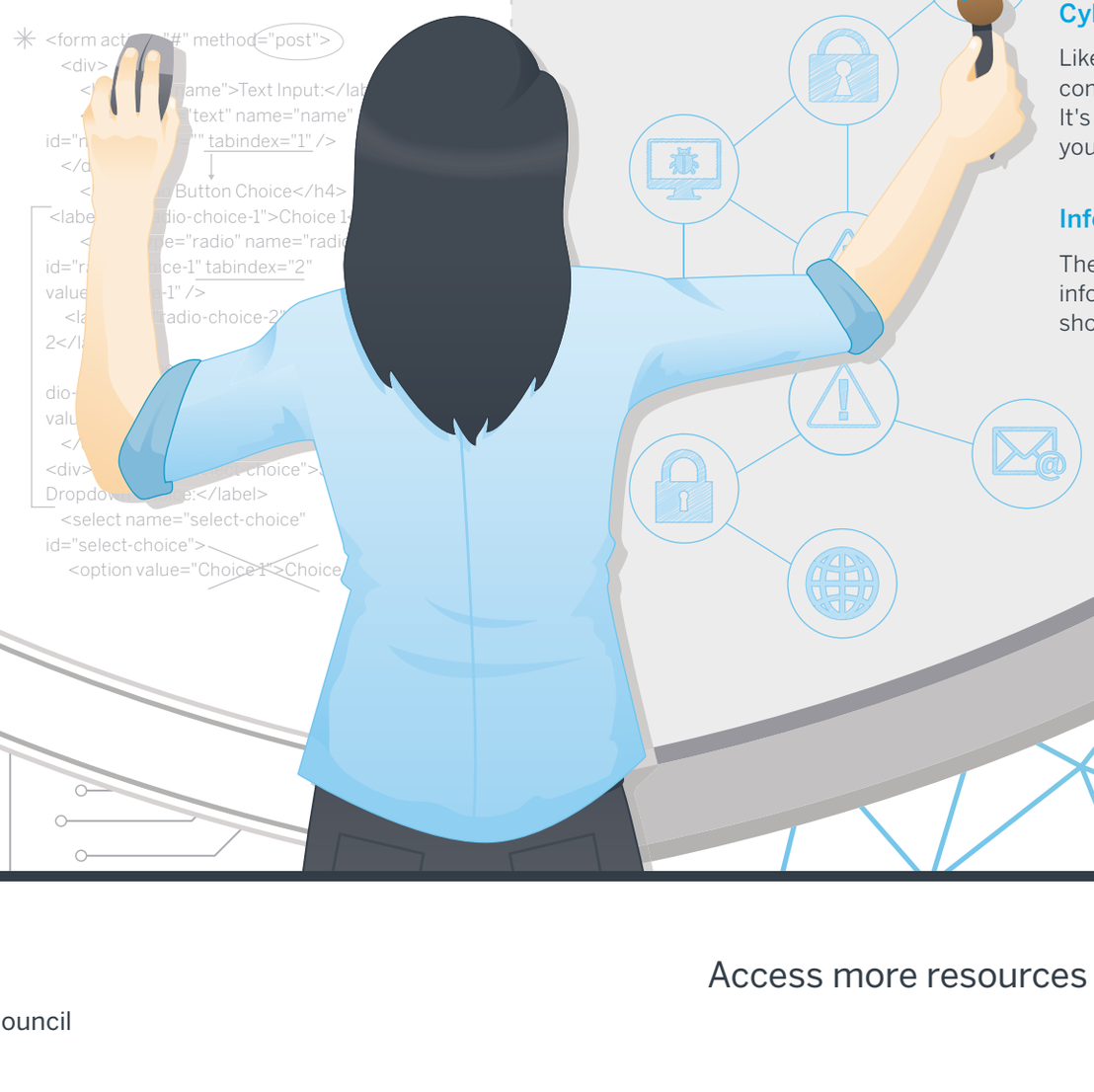
Fully understand what is covered under your plan; carefully consider if it is the best mix of services, liability reduction, and money spent.

Information Sharing

Consider joining a health care information sharing and analysis group to reap the benefits of collaboration and increase security across the industry.

New IT-Enabled Capabilities

Pace technology investments to cover the basics first; supplement with more advanced tools later. Consider tools that preserve or improve clinical workflows.



Cyber Intelligence

Cyber intelligence is your radar into the dark web—advanced warning is valuable.

New IT-Enabled Capabilities

Technology has its limitations. There is no silver bullet for security so beware of any "too good to be true" vendor claims.

Cyber Insurance

Like health insurance, cyber insurance comes with different levels of coverage. It's a way to limit, but not eliminate, your exposure.

Information Sharing

The bad guys continually share information and collaborate. So should the good guys.

1) Business continuity planning.
2) Disaster recovery.
3) Recovery time objectives.
4) Recovery point objectives.

Advisory Board | International Global eHealth Executive Council

Access more resources on information security in health care

advisory.com/geec