Digital Health CANADA | CHIEF Executive Forum

CODE GREY

WHERE SECURITY PRACTICES MEET PATIENT CARE

For healthcare, cyber attacks can have ramifications beyond financial loss and breach of privacy; a cyber attack can bring the delivery of patient care to a halt.

To support the continuity of patient care during and after a cyber incident, this CHIEF Executive Forum resource provides high-level strategic suggestions and trustworthy sources for further information and available tools.

Healthcare delivery organizations can use this to guide them through three key stages of a cyber incident:

Prepare. Respond. Recover.

Prepare.

1. Create a patient care continuity plan specific to cyber risk.

- Implement departmental awareness of all patient safety legislation requirements
- Ensure key clinical offerings/patient care can be delivered with no technology available
- Test both the patient care and incident response plans by practicing worst case scenario drills i.e., there is no IT available, and the crisis must be managed while delivering care & rebuilding technology

2. Create an incident response plan specific to cyber risk.

- Create an incident response plan specific to cyber risk.
- Have the right resources, competencies, and relationships in place with clearly defined incident management roles and responsibilities
- Establish a relationship with the security community and the Canadian Centre for Cyber Security (Cyber Centre)
- Prepare a complete list of stakeholders with legal, communications, forensics, and insurance resources (not just IT)
- Ensure vendors are following your organization's cybersecurity requirements. The Cyber Centre offers guidance on supply chain security at the following two links:
  - Cyber supply chain: An approach to assessing risk - ITSAP.10.070
  - Security considerations when using open source software (ITSAP.10.059)
  - Cyber security considerations for consumers of managed services (ITSM.50.030)

3. Implement executive-level reporting of cybersecurity operational risk.

- Perform an annual external audit
- Have defined accountabilities
- Put into place robust metrics, KPIs, and leading indicators

4. Increase board-level oversight into cybersecurity risk and/or consider forming a cybersecurity committee (separate from any audit/risk committee).

- Create an annual IT risk forecast with an appropriate baseline to measure against
- Put in place security controls (Top 10 security actions, Top Security Enhancement Measures for SMO) similar to financial controls including the review of unsecured third party partners

5. Lead a cybersecurity culture change.

- Endorse a cybersecurity policy tied to the organizational goal of caring for patients and employee well being
- Institute cybersecurity awareness training for all employees and leverage existing Government of Canada training and awareness products
- Balance organizational cybersecurity activities between prevention and response
- Give staff the tools required to: recognize a security incident; understand the obligation to report; and feel comfortable and safe following the reporting procedure.
- Make sure your organization has appropriate cyber hygiene by following the cyber hygiene checklist.

Respond.

1. Respond to a cyber attack with collaboration.

- Teams from cyber incident response and recovery, IT incident management, IT disaster recovery, clinical and non-clinical operations, crisis management, and front-line delivery of patient care must work together.

2. Have a plan. Know the plan. Practice the plan.

- Follow tested patient care continuity and cyber incident response plans. The Canadian Centre for Cyber Security (Cyber Centre) offers several planning resources:
  - Developing your IT recovery plan (ITSAP.40.004)
  - Developing your incident response plan (ITSAP.40.003)
  - Develop an Incident Response Plan: Fillable template and example
- Manage the incident from your pre-established emergency operations centre (EOC)
- Document the incident
- Pre-identify decision makers with the authority to shut down critical systems to prevent further damage

3. Support the incident response with a tested communications strategy that includes action items corresponding to the level of risk.

- Communicate clearly with both internal and external stakeholders
- Communicate with the regional security operations center (SOC) if available
- Set up one communications team for managing the incident and a separate one for updating necessary parties about the incident, including sharing appropriate information with the broader community

4. Metrics and data: collect data to feed into pre-determined metrics

- Collect data to feed into pre-determined metrics* to improve recovery and inform continuous improvement. Recovery metrics can improve specific recovery aspects or contribute to a cost/benefit analysis of a particular approach. Other metrics might be used for compulsory reporting (in response to an inquiry from an external authority) or information sharing.

  *Metrics including but not limited to:
  - **Maximum tolerable downtime (MTD)** The total length of time that a process can be unavailable without causing significant harm to your business.
  - **Recovery point objective (RPO)** The measurement of data loss that is tolerable to your organization.
  - **Recovery time objective (RTO)** The planned time and level of service needed to meet the operational expectations.

5. Report the incident to the the Cyber Centre.

- Report the incident to the the Cyber Centre. Canadian critical infrastructure partners can ask the Cyber Centre for help during a cyber incident. During the containment and eradication phases of an incident, the Cyber Centre Incident Handling team can provide:
  - Advice and guidance • Mitigation and containment
  - Digital forensics and artefact analysis
  - Malware analysis • Tactical threat intelligence
  - Malicious content takedowns

Recover.

1. Have a cybersecurity recovery plan that examines how to effectively respond to new threats and risks. The plan should address:

- Protecting data assets and ensuring threat actor is no longer on the network
- Investigating, collecting, and preserving evidence
- Root cause and post-incident report analysis
- Addressing jurisdictional privacy rules and regulations and actions that might be required
- Sharing learnings with peer organizations (local, regional, national)
- Restoring reputational damage

The Canadian Centre for Cyber Security offers two resources for cybersecurity recovery plans:

- Developing your IT recovery plan (ITSAP.40.004)
- Ransomware: How to prevent and recover (ITSAP.00.099)

2. Collaborate and coordinate with vendors and internal and external stakeholders through prior planning, preparation, and simulation of events.

- Know who you will need to contact before an event occurs
- Establish working relationships with vendors, the security community, and the Cyber Centre
- Ensure supply chain integrity.

The Canadian Centre for Cyber Security offers three resources for ensuring supply chain integrity

- Cyber supply chain: An approach to assessing risk - ITSAP.10.070
- Supply chain security for small and medium-sized organizations (ITSAP.00.070)
- Cyber security considerations for consumers of managed services (ITSM.50.030)

3. Know how you are going to continue providing care while dealing with the incident.

- Operationalize clinical care without digital technology Business Continuity Planning (BCP)
- Perform tabletop exercises that simulate continuing operations while dealing with an incident and how to return to operational capacity

4. Re-evaluate the organization's cybersecurity budget.

- In Canada, the estimated average cost of a data breach (a compromise that includes but is not limited to ransomware) is $6.35M CAD.
- In 2021, the global average total cost of recovery from a ransomware incident (the cost of paying the ransom and/or remediating the compromised network) has more than doubled, increasing from $970,722 CAD to $2.3M CAD.

5. Gather lessons learned to enhance operational resilience and implement changes to prevent recurrence.

- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?
- What types of training programs could the organization implement to ensure all staff members are better prepared?

CODE GREY

Code Grey – Where Security Practices Meet Patient Care provides strategic suggestions your organization can implement to improve cyber security resilience. For more tools and guidance, please refer to the Canadian Centre for Cyber Security website or email them at health-par-sante@cyber.gc.ca

Digital Health CANADA

CHIEF Executive Forum

This resource is the first from Digital Health Canada's CHIEF Executive Forum Cyber Security Working Group, which aims to raise the bar of cyber security in Canadian healthcare organizations and develop a national framework and enhanced guidelines that emphasize people, process, partnerships, and technology working hand in hand. Please visit our website for more information about the CHIEF Executive Forum Cyber Security Working Group