CCTX

CKCA
CANADIAN KITCHEN CABINET ASSOCIATION

Want to Secure Your Business?
Start with Decades Old Cybersecurity Controls

While it may be tempting to focus solely on new and emerging threats, technologies, and strategies [such as zero trust, block chain, network segmentation, AI and machine learning] organizations that prioritize the implementation and maintenance of foundational time-tested cybersecurity controls will be well positioned to protect their digital assets and minimize their risk of cyber incidents.

Despite the ever-evolving landscape of cyber threats and attacks, recommended cybersecurity controls have remained relatively unchanged over the past decade. Many core principles and practices recommended for securing digital assets in 2007 are still relevant today. The COBIT Security Baseline 2nd Edition An Information Security Survival Kit was published in 2007 by ISACA (Information Systems Audit and Control Association)[1].

As documented in the baseline, ensuring staff members have sufficient resources and skills to exercise their security responsibilities is as important today as in 2007. Similarly, establishing clear roles and responsibilities for information security, providing training to operate information systems securely, and ensuring awareness of the need to protect information are all foundational controls that remain critical.

Even the more technically focused control recommendations have not changed that much. However, ensuring they are comprehensively and effectively applied has become critically important. Some of the baseline controls that remain relevant include, but are not limited to:

- Ensure that **physical and environmental protections** (e.g., for heat, dust or electricity) are in place.
- Ensure that important computing equipment is **safe from theft, damage, or loss**, e.g., put cables on laptops, lock computer rooms and know the location of media devices.
- Ensure that **on-call support,** backup, resilience and continuity have been established for IT services supporting critical business functions.
- Ensure that an **up-to-date list of hardware and software** critical for important IT services is maintained, including the disaster backup site.
- Ensure that **archiving and backup procedures** for critical information have been defined and implemented.
- Establish rules for assessing and **authorizing changes** and for evaluating their security impact.
- **Configure basic access control, virus detection and protection, firewalls, intrusion detection, and insurance coverage**.
- **Hardening** all security and critical server and communications platforms.
- Ensure that operating system versions have been continuously kept up to date, i.e. **patching**.
- Ensure that adequate security has been implemented for **wireless** communications systems and is monitored continuously.
- Ensure that risks of dependency on security service providers have been assessed and mitigated; **3rd party risks**.
- Ensure that the usage of computers is **monitored for compliance** with established rules of appropriate usage.

Cont'd…2/

[1] https://books.google.ca/books/about/COBIT_Security_Baseline.html?id=u3CTD5JCSZMC&redir_esc=y

Want to Secure Your Business?
Start with Decades Old Cybersecurity Controls

While there have certainly been advancements in cybersecurity terminology, technology and practices over the past decade, these controls remain the cornerstone of any effective cybersecurity program and serve as the first line of defense against cyber threats and attacks.

For the sake of completeness and to ensure modern practices are considered, small-to-medium sized organizations should consider and align to the Canadian Cyber Centre's *Top measures to enhance cyber security for small and medium organizations (ITSAP.10.035)*.