SAFEGUARDING YOUR CREDIT UNION:

MANAGING COMPLEXITY WITH CELERO'S SECURITY STRATEGY

VERSION 1.0

Table of Contents

State of cyber security in Canada

The growing sophistication of today's cyber attacks leave financial institutions particularly vulnerable. According to Statistics Canada, in 2017, on average, organizations in the Canadian insurance and finance sector were impacted by cyber attacks in the following ways:

- 4 times a year experienced an incident to steal money or demand ransom payment
- 14 times a year experienced an incident to steal personal information or financial information
- 4 times a year experienced an incident to monitor and track business activity

Across the sector, these incidents resulted in a 24 per cent loss of revenue, prevented 61 per cent of employees from carrying out day-to-day work and prevented 62 per cent use of resources or services.

Security threats to financial institutions aren't new – but the level of sophistication, targeting and security circumventions of cyber attackers represent an incredible risk to credit unions' operations, reputation and financial stability.

With the multitude and complexities of these threats, it's become unmanageable, almost impossible, for an individual credit union to have the time, insights, processes and tools to proactively and effectively oversee cyber security on their own. In fact, Verizon's 2018 Data Breach Investigations Report, shows that it generally takes months for a breach to be discovered by an organization.

5 challenges credit unions face

Credit unions in general are likely to have fewer resources and less in-house security expertise, making them attractive targets for cyber-criminals. Add in the following challenges and the need for security as a service becomes clear:

- Credit unions often lack the tools and expertise to effectively get ahead of security threats and compliance risks.
- They are not always able to identify, assess, and mitigate security risks.
- They can detect threats but are unable to respond appropriately in a timely fashion.
- They are unfamiliar with security best practices and the overall threat landscape.
- They can be overwhelmed with the numerous offerings available.

Mobile devices and security

The increase in mobile devices further complicates credit unions' job of securing their environments because mobile devices come with a unique set of security risks, such as fake Wi-Fi networks designed to gain access to data and operating system vulnerabilities.

Mobile devices do not have the same security standards and safeguards as your desktop and are therefore at a greater risk to be attacked. The following graphic shows vulnerabilities and threats of mobile devices in small and medium-sized businesses:

Source: https://www.microsoftpartnercommunity.com/t5/Security-and-Compliance/3-Ways-to-Secure-Small-Business-Customers/td-p/2536

Celero-Microsoft joint security solution

For credit unions, keeping data, workloads, and users secure is more than a full-time job and Celero is helping credit unions avoid becoming a statistic. Credit unions need a reliable expert with extensive experience dealing with security threats, which is why Celero has developed a security baseline for Office 365 leveraging Microsoft Enterprise Mobile Security (EMS) licensing to protect your organization.

Celero's security baseline is a set of configured security controls, specifically set up for credit unions' needs and operations. Using a security baseline reduces the costs and complexity of configuring various security features. Celero offers extensive industry and cloud knowledge to create a tailored experience for your credit union.

Using features from Microsoft EMS, Celero's security baseline has three pillars: securing the front door, secure content and secure devices:

Securing the front door	Secure Content	Secure Devices

• Multi-Factor Authentication (MFA)
• Single sign-on access
• Identity Protection
• Cloud App Security
• Windows Hello
• Office 365 Advanced Threat Protection
  • Advanced Persistent Threats
  • Phishing & Spear Phishing
  • Business Email Compromise (BEC) & Impersonation
  • Malware, Ransomware, Spyware
  • Spam & Graymail
• Advanced Security Management
	• Define policies, templates and rules for content
	• Define exceptions
	• Define content classification labels
	• Monitor and Detect the software as a service (SaaS) apps that are in use and assigning them a security risk rating
	• Define data copy and usage rules for apps on devices
	• Control sharing of data based on identity
	• Detect data and users violating content policies
	• Enable users to take action to maintain content security
		• Conditional Access
		• Device Compliance Policies
		• Device Security Policies
		• App-based Security Policies

Microsoft EMS is an intelligent mobility management and security platform, that enables both security and flexibility for your credit union. There are four key components to the solution to secure identity, devices, data and connections.

Microsoft Azure Active Directory Premium	Microsoft Intune	Microsoft Azure Rights Management Premium	Advanced Threat Analytics
			
Secure Identities	**Secure the Device**	**Secure the Data**	**Secure the Connection**

SECURING IDENTITIES

Faced with the bring your own device (BYOD) trend, IT departments must secure a greater number of devices. Azure Active Directory Premium makes this whole process easier with the following functionalities:

1. Self-service and password reset
2. Multi-factor authentication
3. Single sign-on for multiple apps
4. Threat and security reports
5. Sync capabilities across cloud and on-premises directories

SECURING DEVICES

Employees always want consistent access to the company's resources, from any given device. This is a challenge for IT professionals, who want to provide maximum mobility while protecting the corporate resources. Microsoft Intune is responsible for dealing with the mobile devices of the employees and provides the following functionalities:

1. Mobile application management
2. Support for IOS, Android, and Windows
3. Remote wiping of data
4. Endpoint protection

SECURING DATA

With employees able to remotely access sensitive company data from virtually anywhere in the world, there comes a need for increased protection and security. Frequently, such data need to be shared with colleagues both within and outside the organization. Azure Information Protection offers the following functionalities:

- Classification of data based on sensitivity
- Encryption of data and usage control
- One-click processes that allow employees to protect data
- Reporting and tracking of data

SECURING CONNECTIONS

Through Advanced Threat Analytics, Microsoft secures the whole system of an organization and detects suspicious activities. So that, if the credentials of a manager are compromised and a hacker gains access to the system. Advanced Threat Analytics will warn the company of the potential dangerous situation by detecting the changed behavior of that manager.

Microsoft's Advanced Threat Analytics provides companies with following functionalities:

1. Behavioral analytics
2. Detection and prevention of malicious attacks
3. Alerts and active feedback and recommendations
4. Integration with active Security Information and Event Management (SIEM) systems

5 more reasons to integrate Microsoft EMS

Microsoft EMS reduces the burden on IT teams, which results in cost savings. But what are some of the other benefits of integrating the platform?

MANAGING APPLICATIONS

Microsoft EMS is integrated with more than 2,500 of the leading SaaS applications. This means companies can provide more customized application packages to their users, all with single sign-on enabled.

WORK ANYWHERE, ANYTIME

With a Microsoft EMS system, employees can access their data and applications from literally anywhere in the world. Working from the comfort of your own home has never been easier!

SINGLE SIGN-ON

With single-sign on, employees can access all their registered applications with just a single identity. Ultimately, this simplifies identity management and enhances employee productivity.

DATA PROTECTION

Microsoft EMS is easily integrated with Android, IOS, or Windows operating systems. It provides protection to all these devices and with remote data wiping, usage alerts and notifications, active threat analytics, and data tracking, EMS ensures that all your company data remain protected.

Perhaps the most important benefit of Microsoft EMS is the reduced cost of managing teams. With the platform, the cost of infrastructure decreases, as all data are shifted to the cloud. IT departments also no longer have to worry about micromanaging users. Above all, Microsoft EMS helps companies save considerable sums by reducing the risk of data breaches.

Rely on Celero as your security advisor

As cyber security becomes increasingly complex to manage, financial institutions can rely on Celero to oversee, protect against and prevent security threats. Celero offers robust, managed security services that are continually evolving, improving and growing to meet the challenges of handling cyber security for Canada's financial institutions.

To learn more about how Celero's security baseline and the Microsoft EMS platform can keep your modern, mobile workplace secure, contact Celero for a free demo and consultation.