

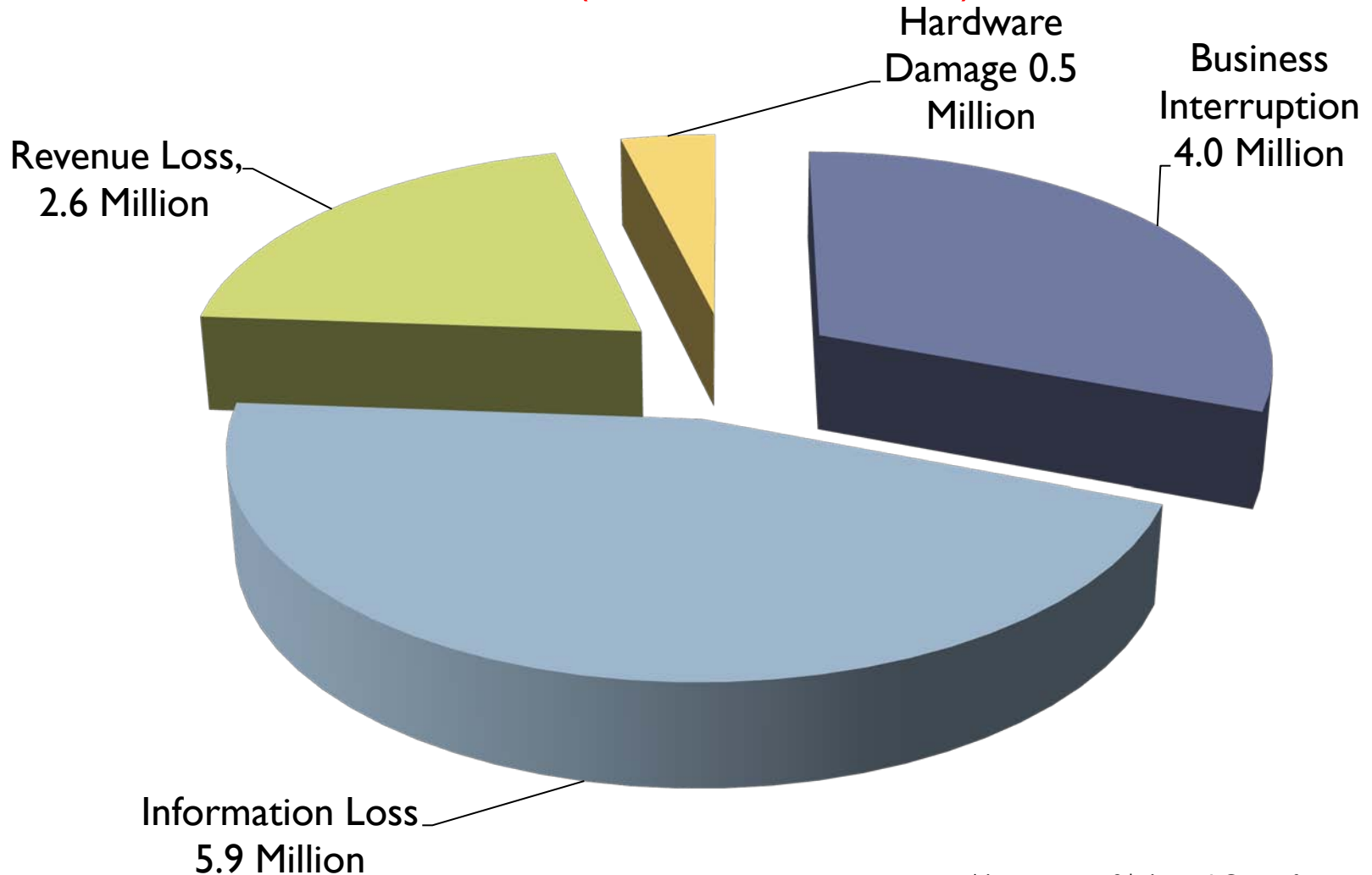


The Cyber Exchange Securing Technology Gaps

By Dan Struthers
HardSoft Systems Ltd
www.hsl.ca



Average Cost of Cybercrime across all 16 countries
Total \$13 Million* (Canada \$ 9.25 M)



*Accenture – 9th Annual Cost of Cybercrime Study – May 2019

Technologies introduce a risk and so do humans












81% Of business leaders say new business models introduce technology vulnerabilities faster than they can be secured

Only 11% Of CISOs say employees in their organizations are held accountable for cybersecurity today

*Accenture – 9th Annual Cost of Cybercrime Study – May 2019



Infrastructure Gap Analysis

								
Hardware	WAN	Anti-Virus Anti-Malware	Intrusion Detection	Local Data Access Control	Data back-up	Off site Back Up	Disaster Business Interruption	People
Trusted Platform	Exposure	Early detection of variants	Server Monitoring	justify access	Oh No (96%)	multi day	Data Facilities Response Plan	Explain their role in Prevention
Protect Physical Access	limit attack surfaces (I.e. print servers)	Ransomware		who is write who is read only	Must be multi day	Test it!!!	Get up and running	Detection
		Passwords			Test it			"hover" over emails
	BYOD policy	"Mary had a little lamb"						look for errors
		better than algorithm						



Technology Gaps That Introduce Risk

▶ **Hardware**

- ▶ Trusted platform
- ▶ Protect physical access

▶ **Network**

- ▶ Exposure
- ▶ Limit attack surfaces
- ▶ BYOD policy

▶ **Anti-Virus / Malware**

- ▶ Early detection of variants / Ransomware
- ▶ Passwords “Mary had a little lamb”

▶ **Intrusion detection**

- ▶ Server monitoring

▶ **Local Data Access Control**

- ▶ Justify access to data
- ▶ Who can write/who is read only? - limits risk to data



Technology Gaps That Introduce Risk

▶ Data Backup

- ▶ Single day or multiple days
- ▶ Oh no!! (96%)
- ▶ TEST the backup on a regular basis



▶ Off-site Backup

- ▶ Multi day – TEST the backup

▶ Disaster Business Interruption

- ▶ Have a written plan to get up and running – TEST it!



▶ People

- ▶ Training
 - ▶ How each employee can be an individual “firewall” – 1st line of defense
 - ▶ How to “hover” over suspicious links and looking at emails in more detail (spelling mistakes)



9 WAYS YOUR EMPLOYEES' WORK CREDENTIALS CAN LEAD TO A BREACH

When your employees use their work email on websites like the ones listed below, it makes your business vulnerable to a breach. With our Dark Web Monitoring, we can detect if your company is at risk due to exposed credentials on 3rd party websites.



HR & PAYROLL



EMAIL SERVICES



CRM



TRAVEL SERVICES



COMMUNICATIONS



E-COMMERCE



BANKING & FINANCE



COLLABORATION



SOCIAL MEDIA



UNDERSTAND & MITIGATE YOUR RISK



THE IMPORTANCE OF DATA BACKUP AND DATA RECOVERY



Thank you

Dan@hardsoft.ca

www.HSL.ca

800 263 8433

