

Let's Talk Cyber Security:

Why We're Vulnerable

www.cymplify.io

Cyberattacks Cost Millions In Damages

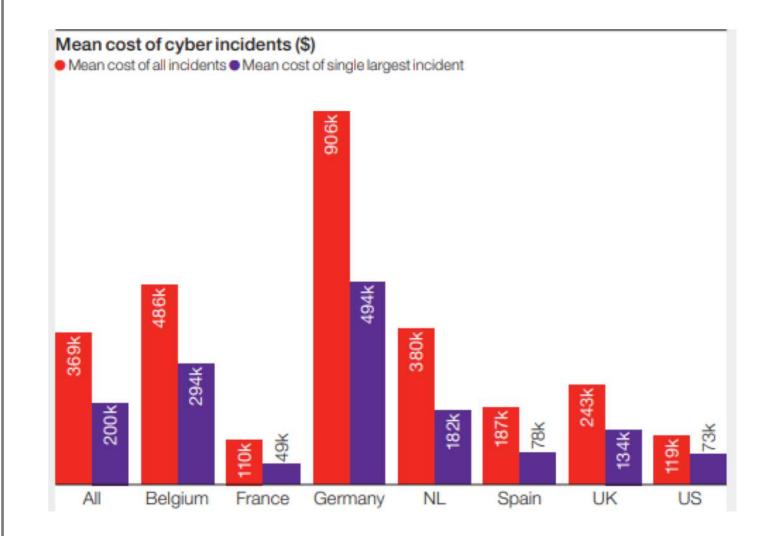
- Maersk (2017) -\$330m lost
- Norsk Hydro (2019) -\$52m lost
- Pilz "Shut down" (2 weeks ago)

DÌZ

MAERSK

German Companies Suffer The Most

(Hiscox Cyber Readiness Report 2019)

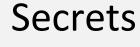


Companies Don't Only Lose Money...



Reputation



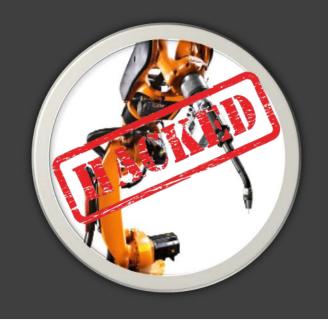
















Regulation is Closing In

California State - SB 327

US GOV - US Internet of Things (IoT) Cybersecurity Improvement Act of 2019

UK - UK's Code of Practice for Consumer IoT Security

EU - ETSI TS 103 645

Who Are We?

- Ex-Elite IDF cyber unit
- Tested on thousands firmwares
- Validated by global Cybersecurity leader
- Integration with several major companies



Protecting The Device Itself

Our solution

End2End Cyber Solution





At customer site

Why We're Different

- Protect the device itself
- Simple use
- Future proof
- Regulation compatible

All rights reserved - This is a property of Schwifty Security Ltd (Cym

Customer Demand = Big Opportunity





Let's Talk

Free Security Report

Ram Yonish, CEO
ryonish@Cymplify.io
972-52-24-24-314

Summary Severe Vulnerabilities Weak Credentials Dangerous Configs 100% 48% 5% Action Items Action Severity Fix vulnerabilities listed in report Critical Change easily-crackable passwords / known passwords High Disable risky Linux Kernel configurations. Disable via kernel config: make menuconfig Enable highlighted Linux Kernel security features. Enable via kernel config: make menuconfig Rebuild ELF binaries using security features. Add compilation flags to gcc: Stack smashing protection: -fstack-protector-all Debug symbols removal: -s Enable ASLR: -fPIE -ple Relocation Read-only: -WI,-z,reiro-WI,-z,now Address Sanitizer: -fsanitize=address. If your toolchain does not contain a libasan.so, this will not work Fortify Source: -D_FORTIFY_SOURCE=2

www.cymplify.io