Continuing to Adapt
Navigating the Evolving Threat of Ransomware

Mark Teolis
Director of TELUS Cyber Resilience and Incident Command

Scope of responsibility

TELUS Business

Managing security for our business customers

TELUS Health

Healthcare tech serving 68 million people

TELUS

35k employees and 18 million telecom customer connections

TELUS Agriculture & Consumer Goods

Supporting 100M acres of agricultural land

TELUS International

73k employees, operating in 30 countries

Keys to a successful technology transformation journey

Our experience in 2023 - volumes and trends

29 trillion
(2X increase since 2020)

Reconnaissance scans against the TELUS network in search of opportunities to attack

65 quadrillion
(5X increase since 2020)

Bits of online traffic attempting to cause outages

1 billion

Email attacks blocked in 2023
▲200M since 2020

4 billion
(3X increase since 2020)

Attacks targeting TELUS websites

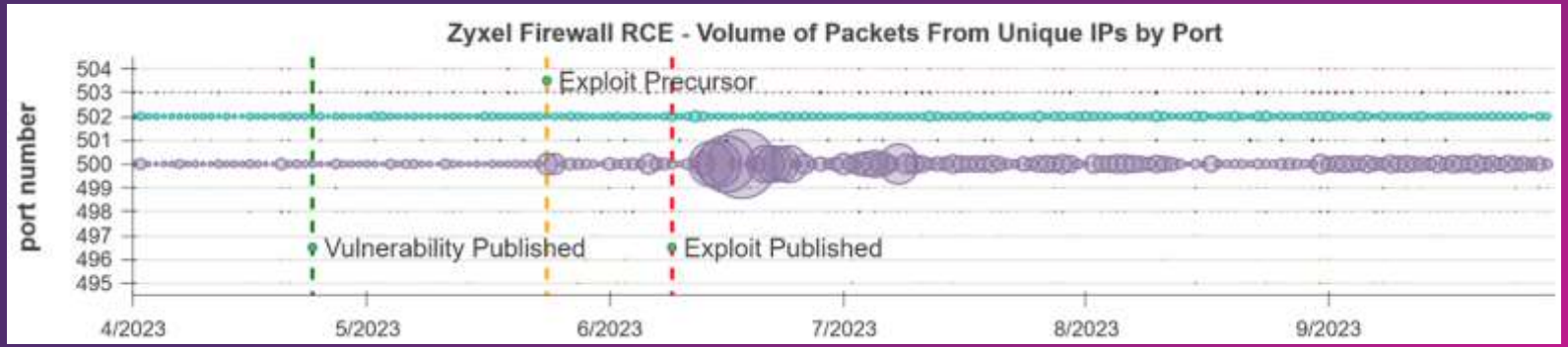
3.5 billion
(2X since 2020)

Attacks attempting to infect TELUS systems with malicious software

Scanning | DDOS | VPN
DLP | EDR | WAF
Firewalls | IDS/IPS | SSE

Our experience in 2023

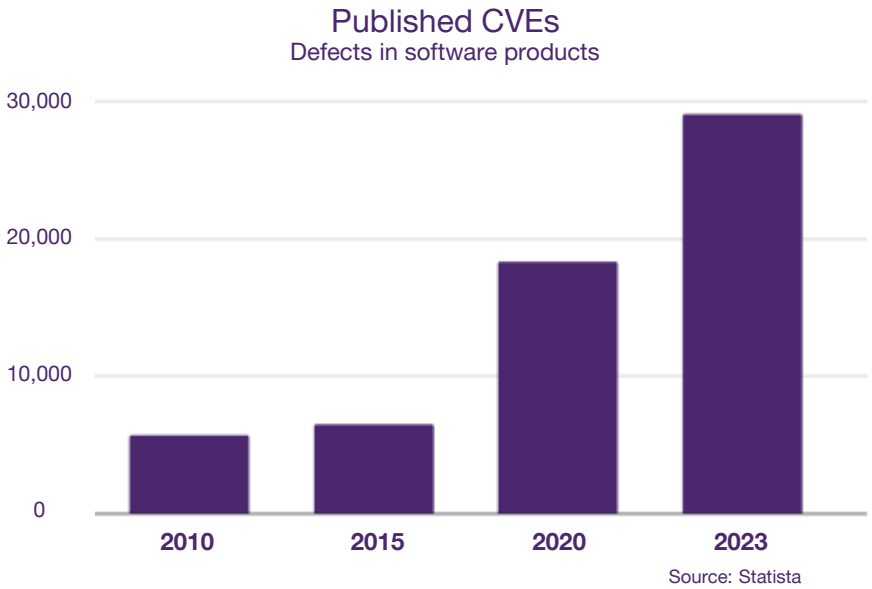
Scanning behavior during vulnerability timeline



Source: TELUS internal

Published exploit for remote unauthenticated command injection in Internet Key Exchange (IKE) packet decoder over UDP port 500
CVE-2023-28771

All trends point to an increasingly challenging environment



TELUS saw an 110% increase in critical vulnerabilities in 2023

Breakout Time

2021	98 mins	
2022	84 mins	-14%

Source: IBM X-Force Threat Intelligence Index 2024

Ransomware deployment timeline

2019	60+ days
2020	9.5 days
2023	~3.9 days

Source: 2023 Crowdstrike Threat Report

TELUS observed attempted ransomware deployment in as little as 2 days in 2023

All trends point to an increasingly challenging environment

Increasing number of attacks	YoY growth in vulnerabilities	Speed of exploit

83%

experienced attempted ransomware attacks*

Top vectors

Misconfigs
Email
Known vulnerabilities
Zero-day
3rd party

143% increase in incidents in Q1 2023**

93% increase in data exfiltration attacks 2019 to 2022**

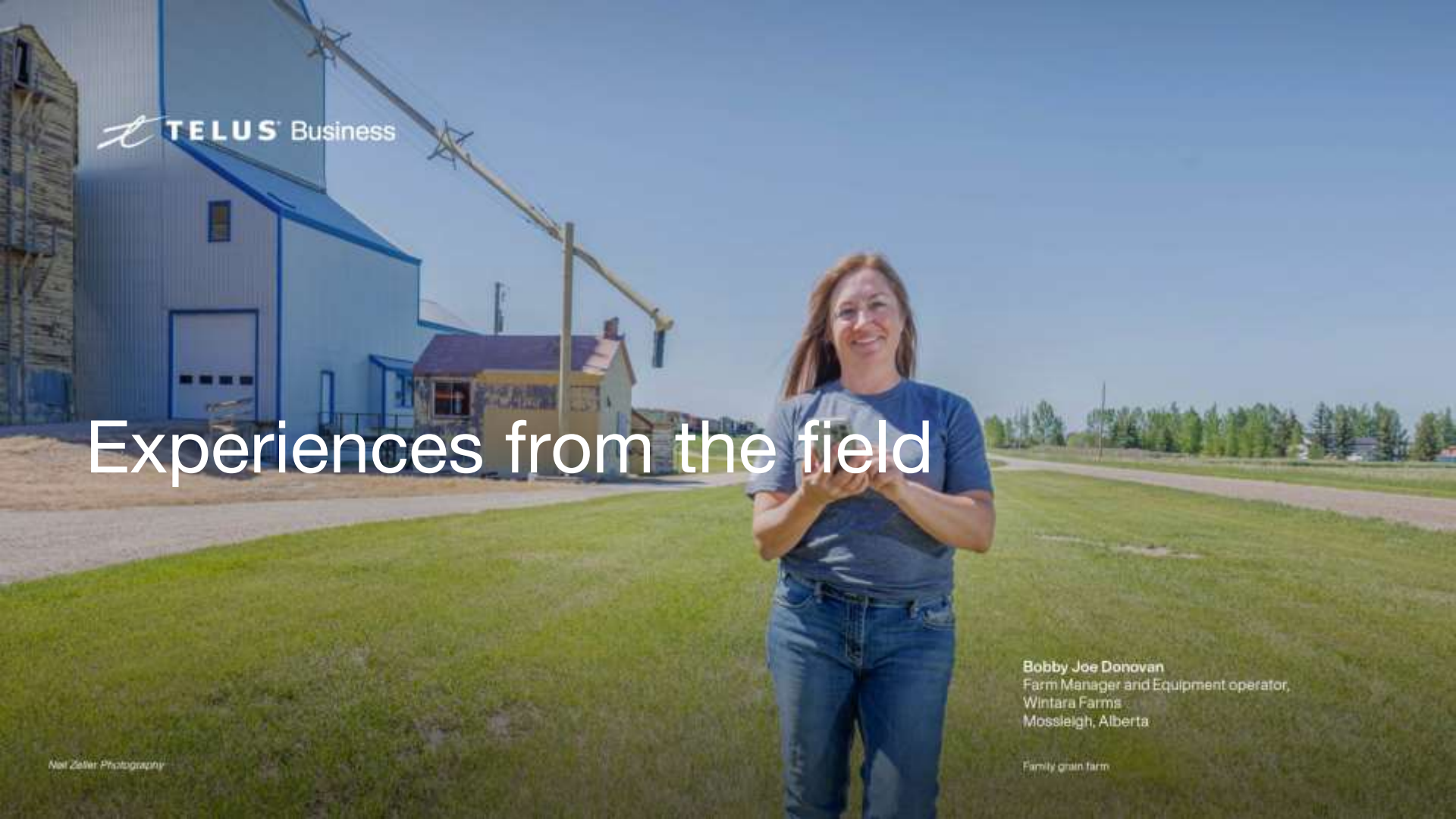
2.5x

increase in likelihood of paying ransom for attacks involving data exfiltration**

24% took weeks to months to contain*

Breaches that are not detected and contained quickly can be 1000x more expensive**

*Source: 2022 TELUS Canadian Ransomware Study
**Source: 2023 Cyber Trends Study, Allianz


TELUS Business
Experiences from the field
Bobby Joe Donovan
Farm Manager and Equipment operator,
Wintara Farms
Mossleigh, Alberta
Family grain farm
Neil Zeller Photography

Experiences from the field: social engineering

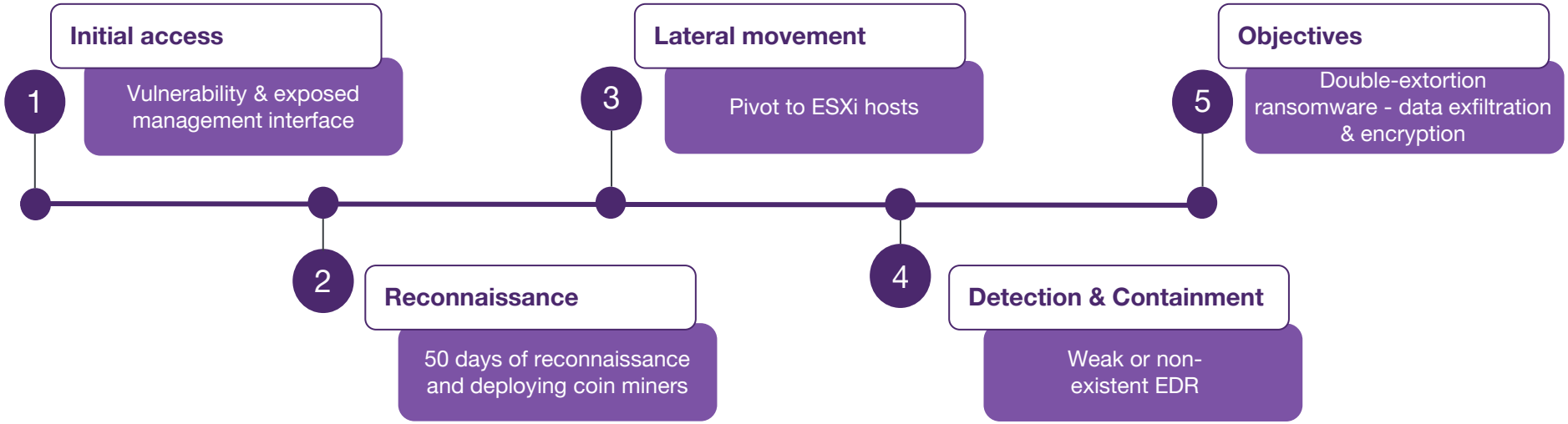
1. Email, SMS or call directing employee to a company SSO page
2. Employee enters credentials/OTP or receives multiple MFA requests
3. TA uses credentials to login and take over employee account
4. Reconnaissance of business processes, documents and systems
5. Objectives / Data exfiltration and / or ransomware deployment

IT Helpdesk support ticket ● Offers of money ● Threats of physical violence

Key learnings

- Phishing-resistant 2FA
- Human firewall and security awareness training
- Threat intelligence & awareness
- Detections focused on identity

Experiences from the field: unpatched vulnerabilities



Key learnings	Unpatched vulnerabilities	Disaster Recovery plans for bare metal (in timely fashion)	Endpoint protection	Network misconfigs	Segmented network security

Experiences from the field: the third party factor

Zero day vulnerability

- Clop group exploited zero-day vulnerability against internet-facing systems running MOVEit file transfer software
- Data was exfiltrated and used for extortion

2700
organizations impacted, many of them as third or fourth parties

Impact
Managing multiple concurrent incidents added strain to responding teams

84 million
people impacted

$100M
estimated in ransoms paid

Key learnings

- Threat intelligence & monitoring of partners
- Third party / supplier security program
- Data mapping and awareness
- Incident response plans for multiple, concurrent ransoms

Organizations need to be cyber resilient

A cyber resilience strategy gives you the ability to withstand and recover from cyber attacks.

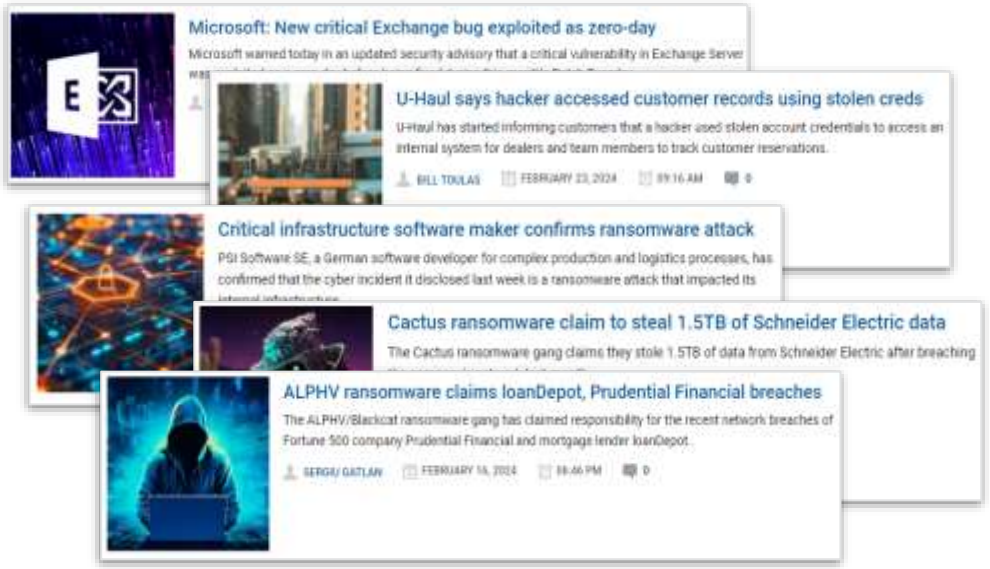
It requires:

Proactive measures

Continuous monitoring, threat intelligence gathering, regular testing and updating security measures

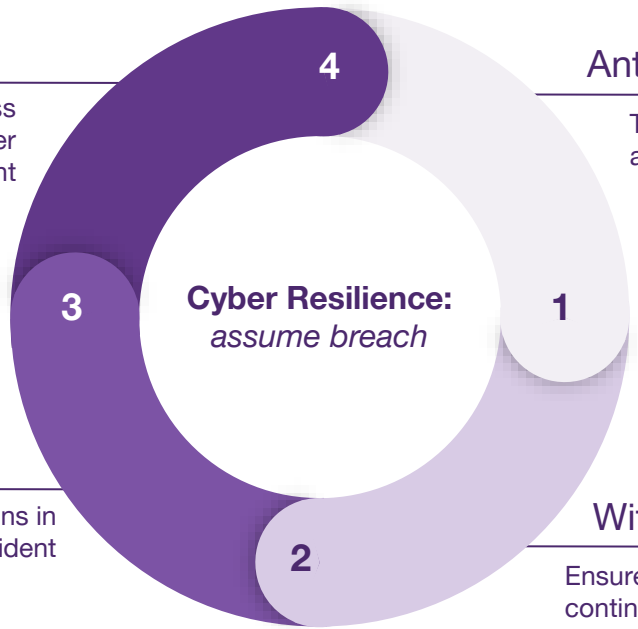
Reactive Strategies

Restoring systems and service, mitigating effects of attacks, relying on incident response and backups to minimize downtime, and financial loss



As evidenced by daily news stories, organizations cannot always prevent attacks - however, they can minimize the impact of attacks that manage to bypass their defense systems

Adapting to this new normal requires a shift in mindset



Adapt

Continuously assess business needs, IT ecosystem and cyber threat environment

Anticipate

Types of adversity (e.g. identity attacks, ransomware)

Recover

Enable restoration of functions in the wake of a cybersecurity incident

Withstand

Ensure essential functions can continue in the face of adversity

PIRs focus on identifying missed opportunities to minimize impact

Cyber resilience is the ability of an organization to withstand, adapt to, and recover from cyber attacks while maintaining essential functions and protecting critical assets.

Maintain a solid foundation of core controls as you evolve towards cyber resilience

Core security controls

Good hygiene and controls that align to modern defense-in-depth and secure-by-design principles

Cyber resilience

Limiting impact from ransomware by adopting strategies to anticipate and recover quickly

Evolving threat landscape

Degrading threat landscape with increasing attack surface, traffic and decreasing exploit time

TELUS Canadian market research

The **TELUS Canadian Ransomware Study** shares insights about how Canadian organizations are tackling the challenge of ransomware.

telus.com/RansomwareStudy

The **TELUS Canadian Cloud Security Study** shares insights on the security challenges of cloud adoption amongst Canadian organizations.

telus.com/CloudSecurityStudy

The **TELUS Canadian Cyber Insurance Study** shares the realities of obtaining and maintaining insurance plus the outcomes of submitting a claim.

telus.com/CyberInsuranceStudy

Studies can also be downloaded using this QR code

Thank you