Cybersecurity evolving Threat Landscape

Paul Ryan
Vice President, Security and Resiliency

Paul Ryan
Vice President
Cyber Security

DELL Technologies

Background & Introduction

Dell Financial Services™	Global Business Unit Security Officer CISO Dell Bank
RBS The Royal Bank of Scotland Group	Corporate CISO: RBS & Ulster Bank
AIB	Head of Cybersecurity Transformation: Retail and Commercial Banking
Integrity360 your security in mind	Chief Strategy Officer and Principal Cyber Consultant

Primer: The Role of Legal in Cybersecurity

Cybersecurity leaders have an ever-growing reliance on multi-disciplinary Legal teams and here’s why:

Cyber Threat Management

- Data breach response
- Commercial Espionage
- Incident Response
- Investigation of incidents
- Cyber crime prosecutions
- Insider Risk and Fraud
- eForensics

Governance

- Setting corporate policy
- Setting Risk Appetite
- Third Party Risk Management
- Cybersecurity disputes
- Ransomware Payment
- Setting strategy
- Board briefing

Compliance and Regulation

- Retention Policy
- Global regulatory compliance
- Intellectual property
- Industry standards (ISO, Sox)
- Training and awareness
- Security audits
- Regulatory audits

Partnership

Cybersecurity is no longer simply an IT department’s problem and, in fact, cannot be the responsibility of any single department.

DELL Technologies
Security & Resiliency Organization

Case Study:

Threat Landscape and Cyber Resiliency

Cybersecurity Concerns

Disrupted operations

Data theft/ breach

Financial impact

Business reputation

UNCERTAINTY

65%

Of IT decision makers are not very confident their data/systems can be fully recovered.[1]

COMPLEXITY

10x

Organizations are managing 10x the data vs. 5 years ago — almost 15 PB on average now.[1]

VULNERABILITY

60%+

of organizations have experienced a data loss due to an exploited vulnerability.[2]

1. Dell Technologies Global Data Protection Index, September 2021
2. Forrester Consulting Thought Leadership Paper Commissioned by Dell, BIOS Security – The Next Frontier for Endpoint Protection, June 2019

The Evolving

Threat Landscape

Every 11 seconds

A cyber or ransomware attacks occur[1]

$6T

Total global impact of cyber crime in 2021[2]

$13M

Average cost of cybercrime for an organization[3]

Recent Global Ransomware Attacks

HSE Feidhmeannacht na Seirbhíse Sláinte Health Service Executive	**May 14, 2021:** the Health Service Executive (HSE) of Ireland suffered a major ransomware cyberattack which caused all of its IT systems nationwide to be shut down
The Indian EXPRESS	**Mar. 21, 2022:** The Maharashtra Industrial Development Corporation (MIDC) said it was the victim of a ransomware attack
REUTERS	**Feb. 27, 2022:** Japan's Bridgestone reports ransomware attack at U.S. subsidiary
CPO MAGAZINE	**Feb. 23, 2022:** Gaming Chipmaker Nvidia confirmed a data leak after a suspected ransomware attack hit the company
Forbes	**Feb. 13, 2022:** San Francisco 49ers was hit by the BlackByte ransomware gang, which claims to have stolen private data
coindesk	**Nov 10, 2021:** Europe's largest electronics retailer MediaMarkt hit by ransomware demand for $50M Bitcoin payment
CNBC	**May 7, 2021:** Colonial Pipeline paid $5 million ransom one day after cyberattack

*[1]Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021 https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

[2]Cybersecurity Ventures: *https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021*

[3]Accenture Insights, Ninth Annual Cost of Cyber crime Study March , 2019 - https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

DELL Technologies

Cyber Resilience: Legal and Regulatory Trends

"An air-gapped data backup architecture…"

Federal Financial Institutions Examination Council

"Confidentiality, integrity, availability and resilience"

General Data Protection Regulation

"It is critical to maintain offline, encrypted backups of data"

Federal Financial Institutions Examination Council

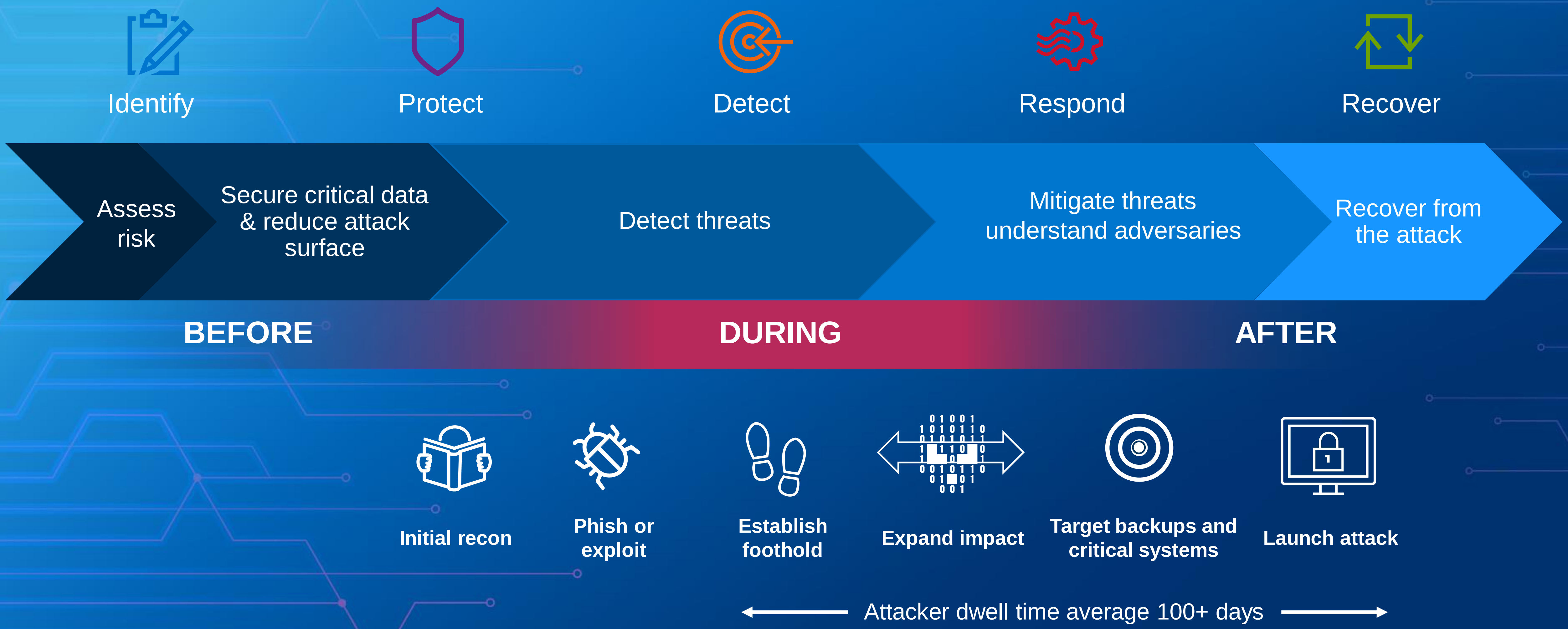
"Ransomware payments may risk violating OFAC regulations"

The Department of the Treasury

"Ensure backups are not connected to the networks they back up."

Department of Justice

Resiliency strategy vs attack strategy



Identify

Protect

Detect

Respond

Recover

Assess risk

Secure critical data & reduce attack surface

Detect threats

Mitigate threats understand adversaries

Recover from the attack

BEFORE

DURING

AFTER

Initial recon

Phish or exploit

Establish foothold

Expand impact

Target backups and critical systems

Launch attack

← Attacker dwell time average 100+ days →

NIST Cyber Security Framework

Understanding the motivation is key to evaluating the threat landscape

Nation-state

Traditional espionage that has moved into the cyber domain, disinformation campaigns, destructive attacks.

Organized Crime

Profit-motivated, looking to monetize access and/or stolen information

Hacktivist

Issue-motivated, aiming to distract, expose, embarrass or inflict public harm

Insider Threat

Involves theft of IP/trade secrets, competitive analysis, and/or prospect, customer, or market information

Cyber Resiliency Preparedness

Resiliency Readiness

- Update business continuity plans (systems, third parties, personnel, regionally)
- Reduce single points of failure

Proactive Risk Reduction Measures

- Reduce rights and access of personnel, systems, third parties;
- Reduction of information (physical and digital) in conflict zones
- Increase insider risk monitoring
- Consider what actions can’t be remotely taken if/once RU-net is down

Preparatory Creation of Reactive Levers

- Pre-staged network disconnect/segmentation automation scripts
- Pre-staged identity and access demotions
- File-level mobile asset encryption (beware cached credentials)
- Pre-staged scripts to wipe remote infrastructure (router/infra secrets files, endpoints, clients, etc.)

Crisis Management

- Pre-identified decision automation thresholds and decision rights
- Establish call chains with secondary/tertiary stakeholders
- Retained specialists – legal, communications, incident response surge, etc.

General Preparedness

- Air-gapped and immutable critical backups of data
- Pre-staged white room technology (AD, infra, critical clients, etc.)
- Prioritized restoration playbooks
- Surge recovery staff capability

DELL Technologies

International Cybersecurity Guidance

Be prepared to isolate critical infrastructure from the internet and internal networks

Ensure that software on all devices is up to date, key business systems are patched

Ensure everyone knows how to report phishing emails

Maintain offline, encrypted backups of data

Ensure antivirus software and firewall is installed and check activity regularly

Ensure passwords are strong and unique, enable multi-factor authentication (MFA)

Ensure effective and secure backups are in place and are operating correctly

Check that your incident response plan is up to date

Check that records of your external internet-facing footprint are correct and up to date

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

SANS

National Cyber Security Centre

National Cyber Security Centre

CISA CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Australian Government Australian Signals Directorate

ACSC Australian Cyber Security Centre

CANADIAN CENTRE FOR CYBER SECURITY

DELL Technologies

Takeaway: Set Risk Management Goals

- What are your most important assets and business services?
- What risks do they face and what controls mitigate those risks?
- Are controls continuously measured as operating within expectations?
- What residual risks remain and who at what level has decided those are acceptable?
- Do those risks correspond to the goals of your organisation & strategy?

DELL Technologies