

# 1:

# CYBERSECURITY CONTEXT & BACKGROUND



Cybercrime alone costs nations more than \$1 trillion globally, far more than the record \$300 billion of damage due to natural disasters in 2017. We ranked cyberattacks as the biggest threat facing the business world today — ahead of terrorism, asset bubbles, and other risks.”<sup>2</sup>

Paul Mee & Til Schuermann  
Harvard Business Review

## Cybersecurity in a Technology Dependent Society

**In today's always-on, always-connected economy, businesses are under pressure to enhance their cybersecurity strategy and prove to their customers that data protection is critical to their customer engagement strategy.**

As the world economy continues to digitise operations, supply chains, business transactions, and employee and customer services, cyberattacks are expected to continue to pose as one of the major threats to the world.

With 'Cyberattacks' and 'Data Fraud and Theft' taking 3rd and 4th place on the World Economic Forum 2018 list of Global Risks, the spotlight is on organisations to ensure critical information remains secure and private <sup>3</sup>.

The number of attacks is growing exponentially with hacking and malware accounting for 48% and 30% of attack tactics <sup>4</sup>. The likelihood that all malware will be discovered before harm is done is low, and the discovery time for an attack is on average 197 days <sup>5</sup>.

This time gap provides opportunity to map the network, escalate privileges and plan a devastating attack, ranging from extortion (ransomware) to outright destruction of business-critical systems. These types of cyberattacks can disrupt a business, leading to costly remediation, revenue loss, negative publicity, and lasting customer distrust.

The average cost of a data breach is \$3.86 million, an increase of 6.4% compared to 2017 <sup>5</sup>. The likelihood of a breach recurring over the next two years is 27.9%.

Even with the most sophisticated security solutions, cyber criminals are constantly learning from previous attacks and exploiting vulnerabilities. With continued advancements in machine learning capabilities, the threat of an attack should not be ignored.

The following sections outline some of the motives behind cyberattacks, the types of cyberattacks and how they intrude on your business, and some of the common points of entry.

# Cyberattacks Motives



## Financial

76% of breaches are financially motivated <sup>6</sup>.

In particular, there has been a huge increase in ransomware, with attackers entering an organisation's systems to take control, sending alerts to users to notify them that their data has been ceased until receipt of ransom fee.



## State Sponsored

Governments have quickly realised that cyberattacks are quicker, cheaper and easier than traditional warfare methods.

With potentially detrimental impacts to society, and even harder to detect methods of manipulation, government entities are exploring the creative ways to infect a rival state's society.



## Intelligence Gathering

Cybercriminals leverage the practice of scanning, monitoring, collecting, and exfiltrating sensitive information in order to extort, blackmail or gain advantage over a rival business.



## Hacktivism

The use of computers and computer networks to promote political or social change.

Hacktivist groups such as WikiLeaks & Anonymous have shed light on some of the social injustices that exist in the world and demand those responsible, be held accountable for their actions. Hacktivism accounted for 4.7% of cyberattacks in 2017 <sup>7</sup>.



## Terrorism

Politically motivated extremist groups and non-state actors using computers to cause harm or fear pose a major threat to critical infrastructure,

Financial services, military, energy, utilities, transportation and government offices are highly attractive targets.

# Types of Cyberattack

On average, advanced cyberattacks go 197 days undetected <sup>5</sup>.

Being aware of how cyberattackers infect systems can help your business detect abnormal activity and potentially help detect an attack early on.

Here are some of the common types of cyberattack:



### Malware

Malware refers to the practice of deploying malicious software, including ransomware, spyware, viruses and worms to infect and breach a network.

This can result in blocked access to files and systems, criminals covertly obtaining sensitive information, and disruption to service, amongst others.



### Data Integrity

Malicious data manipulation can be detrimental to a business. This is a highly sophisticated, and easily undetectable cyberattack that causes users to doubt the accuracy of their information. Manipulating public opinion through smear campaigns or changing information in a medical system are two examples of how this type of attack poses a huge threat to society.



### SQL Injection

Deploying malicious code into an SQL-based server can force the server into revealing information it wouldn't normally reveal. This type of attack can allow attackers to tamper with services enabling them to pose as other individuals, void transactions, change data, destroy data and approve administrative access to users.



### Distributed Denial of Service

This type of attack uses multiple compromised systems to attack servers, networks, and systems to flood and exhaust resources forcing the network to fail and deny service to legitimate users.



### Snooping

Similar to the act of eavesdropping, snooping is the practice of unauthorised access to systems and data. This can include monitoring of keystrokes, passwords, login information, communications, webcams etc.



### Cyber-Collection

Used by nation states to conduct espionage and even corporate spies to gather intelligence on rivals, cyber collection is similar to snooping but is with the intention to scan, collect and exfiltrate sensitive information. An example of this is the famous Stuxnet computer worm first uncovered in 2010.

# Points of Entry

Being aware of vulnerable points of entry will help protect the business.

Here are some common points of entry for cybercriminals:



## Insider

28% of cyberattacks come from an insider with legitimate access (4). These attacks are particularly hard to guard against.



## Web Browser

Browsers are constantly connecting users to the outside world. These browsers rely on plugins (Flash, JavaScript etc.), but like other software, these plug-ins come with security flaws that cybercriminals love to take advantage of. 64% of companies have experienced web-based attacks. (8) Perhaps more worryingly, 77% of compromised attacks in 2017 were file-less. (9)



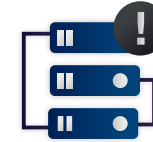
## Phishing Emails

Arguably the most commonly used point of entry, phishing exploits the naivety of users by sending emails that appear to be from a reputable source but contain malicious software. These emails require users to engage with a link or a login portal etc. for the software to be deployed.



## Social Media Platforms

Third party applications, instant messaging services and comments sections are all quick ways for cybercriminals to deploy malicious software to vulnerable users.



## Outdated Infrastructure

It is crucial to update and patch infrastructure. As technology continues to rapidly accelerate and develop, cybercriminals will look to exploit legacy infrastructure. In 2018 outdated security controls was the 2nd greatest vulnerability. (11)



## Unused Systems

Cybercriminals target unused systems and resources because they typically aren't monitored and it's easier to go undetected for longer.



## Zero-Day Exploit

When network vulnerabilities are announced, cybercriminals will actively seek opportunities to exploit this before a patch is issued and implemented.



## Social Engineering

Exploiting the human element of IT, cybercriminals seek to deceive, manipulate, or intimidate people to hand over information and gain access to information systems. In 2017, 43% of cyberattacks involved social engineering. (10)





## Dell Technologies Security Transformation

Dell Technologies unites seven technology leaders in one company with the power to drive digital and security transformation.

Dell Technologies provides a wide range of cybersecurity solutions underpinned by a robust cybersecurity delivery methodology.

Dell Technologies' cybersecurity framework is focused on ensuring our clients manage cyber risk to grow and protect business value.

# Dell Technologies



Dell EMC

Pivotal

RSA

Secureworks

virtustream

vmware



## Dell Technologies Cybersecurity Capabilities

Dell Technologies deliver the following capabilities to our clients:



DELL EMC

Pivotal

RSA

Secureworks

virtustream

vmware

**Deep expertise** across the technology stack from the datacentre right through to end-user devices

**International cyber skills** and leading capability in cyber, digital trust and IT transformation

**A focus on continued R&D** in cyber, digital security and trust

**A world class threat intelligence network** that leverages machine learning and deep learning technologies

**Commitment to a wider ecosystem** of partners that leverages leading edge cyber innovation

**Shared commitment to sustainability** delivering technology solutions that are sustainable and low carbon



# Dell Technologies Cybersecurity Delivers Key Business Outcomes

## Dell Technologies Cybersecurity Capabilities:

Deep expertise

International cyber skills

A focus on continued R&D

A world class threat intelligence network

Commitment to a wider ecosystem

Shared commitment to sustainability

## Dell Technologies Cybersecurity Methodology



Leverage World Class Threat Intelligence Network

## Business Outcomes and Deliverables Include:

 DEFINED STRATEGY AND ROADMAP

 ADVANCED PROTECTION

 RISK AND COMPLIANCE LEADERSHIP & CULTURE

 OPERATIONAL RESILIENCE

 REAL TIME VISIBILITY OF EMERGING THREATS

Our proven methodology is supported by a portfolio of leading cybersecurity solutions that protect and secure your IT environment.

# Dell Technologies Security Transformation Portfolio

Our methodology is enabled by our robust portfolio of cybersecurity solutions.



## Assess Environment & Define Strategy

We assess our clients cybersecurity landscape and we work with them to define cyber strategies and actionable roadmaps in line with strategic objectives.

**Solutions include:**

- Maturity Assessment
- Adversarial Testing
- Cloud Security Consulting



## Implement Strategy & Secure Environment

We implement cybersecurity products and services in line with business objectives to drive growth, protect value and stay on top of cyber threats.

**Solutions include:**

- Infrastructure Security
- Application Security
- End-User Devices Security
- Governance, Risk, Compliance & Controls Operations



## Respond & Recover

We ensure our clients always have measures in place in the event of an attack.

**Solutions include:**

- Threat Detection & Response
- Incident Response
- Cyber Recovery Solution

## Leverage Advanced Threat Intelligence

We provide real time threat data to equip security teams to proactively detect and manage cyber threats and respond more effectively to cyber incidents.

# Dell Technologies Cybersecurity Solutions Deliver Business Outcomes

In this document, we outline some of our leading cyber solutions. This diagram illustrates which solutions deliver the relevant business outcomes.



## Delivery Models

Dell Technologies cybersecurity solutions are categorised under the following delivery models:



### ASSESSMENT SOLUTIONS

These include solutions that determine the risk maturity, exposure and future cyber strategy and roadmap.



### MANAGED SERVICE SOLUTIONS

These include solutions that are provided by Dell Technologies' Managed Service capability on behalf of our clients.



### PRODUCT SOLUTIONS

These include solutions that can be deployed and embedded within a client environment to protect, secure and build resilience.

### Working in Partnership with Consulting Firms

We work with leading Advisory, Consulting and Partner firms to support clients to deliver successful security transformation, risk management and cyber strategy programmes.


## Contact Details

 [www.DellTechnologies.com](http://www.DellTechnologies.com)

 [@DellTech](https://twitter.com/DellTech)



**Dayne Turbitt**  
Senior Vice President UKI

 [Dayne.Turbitt@Dell.com](mailto:Dayne.Turbitt@Dell.com)

 [bit.ly/2xGgo0p](https://bit.ly/2xGgo0p)



**Margarete McGrath**  
Chief Digital Officer UKI

 [Margarete.Mcgrath@Dell.com](mailto:Margarete.Mcgrath@Dell.com)

 [bit.ly/2NGJdUq](https://bit.ly/2NGJdUq)




**Chris Miller**  
RSA Regional Director, UKI

 [Chris.Miller2@RSA.com](mailto:Chris.Miller2@RSA.com)

 [bit.ly/2V9TI82](https://bit.ly/2V9TI82)



**Simon Godfrey**  
Secureworks Regional Director, UKI

 [SGodfrey@Secureworks.com](mailto:SGodfrey@Secureworks.com)

 [bit.ly/2V5J3pD](https://bit.ly/2V5J3pD)

The Dell Technologies logo is centered on a dark gray background. It features the word "DELL" in a bold, white, sans-serif font, with a stylized "E" that has three horizontal bars. To the right of "DELL" is the word "Technologies" in a lighter, white, sans-serif font. The background is decorated with a network of thin white lines connecting various sized gray circular nodes, creating a complex web-like pattern that extends across the right side of the image.

DELL Technologies