Surfing the wave of destructive Cyberattacks
—
Felicity March
Cyber Resilience Specialist, IBM
Cyber Resilience is the ability of an organisation to maintain its core purpose and integrity during and after a cyber attack.

Cyber Resilience needs an end-to-end approach that brings together critical areas to ensure organisations continue to function during cyber attacks and cyber outages.

Cyber Security

Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects organisations from the deliberate exploitation of their assets.

Business Continuity

Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for business continuity address natural catastrophes, accidents and deliberate physical attacks; but now they must also support resumption of operations following cyber attack disruptions.
Cyber Resilience is the ability of an organisation to maintain its core purpose and integrity during and after a cyber attack.

Cyber Resilience needs an end-to-end approach that brings together critical areas to ensure organisations continue to function during cyber attacks and cyber outages.

Cyber Security

Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects organisations from the deliberate exploitation of their assets.

Business Continuity

Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for business continuity address natural catastrophes, accidents and deliberate physical attacks; but now they must also support resumption of operations following cyber attack disruptions.
Cyber Resilience

Cyber Resilience is the ability of an organisation to maintain its core purpose and integrity during and after a cyber attack.

Cyber Resilience needs an end-to-end approach that brings together critical areas to ensure organisations continue to function during cyber attacks and cyber outages.

Cyber Security

Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects organisations from the deliberate exploitation of their assets.

Business Continuity

Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for business continuity address natural catastrophes, accidents and deliberate physical attacks; but now they must also support resumption of operations following cyber attack disruptions.
Cyber Resilience
What’s the impact?
Cyber Resilience Assessment

Work out your vulnerabilities and build a safe future proof strategy

Identify
- Identify your risks

Protect
- Protect your assets against attacks

Detect
- Detect threat activity

Respond
- Respond with a Plan

Recover
- Recover normal operations

Source: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)
IBM Global Technology Services / © 2019 IBM Corporation
The cost of cyber attacks is more than 3x the cost of natural disasters.

**Source:** '2018 Cost of Data Breach Study: Impact of Business Continuity Management' – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018
cyber attacks occur everywhere, including areas that are generally safe from natural disasters.

Source: '2018 Cost of Data Breach Study: Impact of Business Continuity Management' – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018
Organisations are unprepared

What percentage of organisations lack the ability to remain resilient in the wake of a cyber attack?

38%

68%

Source: '2018 Cost of Data Breach Study: Impact of Business Continuity Management' – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018

IBM Global Technology Services / © 2019 IBM Corporation
Organisations are unprepared

What percentage of organisations lack the ability to remain resilient in the wake of a cyber attack?

38%

68%

Source: ‘2018 Cost of Data Breach Study: Impact of Business Continuity Management’ – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018
Organisations are unprepared

What is the average number of days an organisation needed to contain a cyber attack?

69 days

99 days

Source: '2018 Cost of Data Breach Study: Impact of Business Continuity Management' – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018
Organisations are unprepared

What is the average number of days an organisation needed to contain a cyber attack?

69 days

99 days

Source: '2018 Cost of Data Breach Study: Impact of Business Continuity Management' – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018
Organisations are unprepared

What is the average number of days hackers spend inside IT environments before discovery?

97 days

197 days

Source: '2018 Cost of Data Breach Study: Impact of Business Continuity Management' – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018
Organisations are unprepared

What is the average number of days hackers spend inside IT environments before discovery?

97 days

197 days

Source:  ‘2018 Cost of Data Breach Study: Impact of Business Continuity Management’ – Benchmark research sponsored by IBM Independently conducted by Ponemon Institute LLC, October 2018
True Impact

How much was wiped from the share price of a single company by the 2017 NotPetya attack

$370m

$870m

Source: ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’ – Andy Greenberg, Wired.com, August 2018

IBM Global Technology Services / © 2019 IBM Corporation
How much was wiped from the share price of a single company by the 2017 NotPetya attack

$370m

$870m

Source: ‘The Untold Story of NotPetya, the Most Devastating Cyberattack in History’ – Andy Greenberg, Wired.com, August 2018
How many NHS appointments were cancelled due to the The WannaCry ransomware cyber attack?

15k

19k

Source: "This is how much the WannaCry ransomware attack cost the NHS" – Danny Palmer, ZDNET October 2018
How many NHS appointments were cancelled due to the The WannaCry ransomware cyber attack?

Source: "This is how much the WannaCry ransomware attack cost the NHS" – Danny Palmer, ZDNET October 2018
But it doesn’t have to be like this...
Cyber Resilience is the ability of an organisation to maintain its core purpose and integrity during and after a cyber attack.

Cyber Resilience needs an end-to-end approach that brings together critical areas to ensure organisations continue to function during cyber attacks and cyber outages.

Cyber Security

Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects organisations from the deliberate exploitation of their assets.

Business Continuity

Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for business continuity address natural catastrophes, accidents and deliberate physical attacks; but now they must also support resumption of operations following cyber attack disruptions.
Cyber Resilience is the ability of an organisation to maintain its core purpose and integrity during and after a cyber attack.

Cyber Resilience needs an end-to-end approach that brings together critical areas to ensure organisations continue to function during cyber attacks and cyber outages.

Cyber Security
Cyber security is designed to protect systems, networks and data from cyber crimes. Effective cyber security reduces the risk of a cyber attack and protects organisations from the deliberate exploitation of their assets.

Business Continuity
Business continuity provides the capability to resume operations when an event causes a service disruption. Plans for business continuity address natural catastrophes, accidents and deliberate physical attacks; but now they must also support resumption of operations following cyber attack disruptions.
Cyber Resilience
What’s the impact?

Cost
Time to recover
Reputation
BAU
Are you prepared?

If this were happening to your organisation which scenario would it most resemble?

scenario 1

scenario 2
Cyber Resilience Assessment

Work out your vulnerabilities and build a safe future proof strategy

- Identify risks
- Protect your assets against attacks
- Detect threat activity
- Recover normal operations
- Respond with a Plan

Source: [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)
Cyber Resilience Assessment

Roadmap

Cyber Resilience Program
A formal, executive-driven charter to help manage cyber threats across the organisation

Cyber Resilience Risk Assessment
To understand inherent risks, exposure, liabilities; design appropriate plans; Prepare Enterprise Blueprint

Acquire Capabilities
Evaluate & Acquire Technical capabilities based on the Risks; integrate, implement solutions

Continuous Improvements
Test & Rehearse; change & update; conduct training & awareness programs
Thank you

Felicity March
Cyber Resilience Specialist, IBM
@FlickMarch
linkedin.com/in/FelicityMarch