

Building Cyber Resilience

Barbara Brivio
Data Protection Solution Channel lead Italy&Iberia

 Dell Technologies

Cyber threats 2021: the facts



Every 11 seconds

A cyber or ransomware attacks occur¹



\$6T

Total global impact of cyber crime
in 2021²



\$13M

Average cost of cybercrime for
an organization³

Banking	\$18.4M
Utilities	\$17.8M
Software	\$16.0M
Automotive	\$15.8M
Insurance	\$15.8M
High Tech	\$14.7M
Capital Markets	\$13.9M
Energy	\$13.8M
US Federal	\$13.7M
Consumer Goods	\$11.9M
Health	\$11.9M
Retail	\$11.4M
Life Sciences	\$10.9M
Media	\$9.2M
Travel	\$8.2M
Public Sector	\$7.9M

¹Cybersecurity 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>

²Cybersecurity Ventures: <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021>

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

Cyber attacks – a threat to Transformation

Data-driven Society

Data has immense value, offers insights and transfers leverage.
Data fuels Global economies and our professional, social and individual lives

Inadequate Protection for Critical Data

Cybercrime and cyber warfare are outpacing preventative solutions and are terminal threats to businesses, Governments and all data-driven entities

Cyber Recovery is an Enabler of Security Transformation

Modern threats require modern protection, isolation and intelligence to enable recovery in wake of successful ransomware or cyber attack

"64% of Global IT decision makers are concerned that they will experience a disruptive event in the next twelve months"¹

Global Data Protection Index Survey 2021 Snapshot

"67% of Global IT decision makers are not very confident that all business critical data can be recovered in the event of a destructive cyber attack."¹

Global Data Protection Index Survey 2021 Snapshot

¹Based on research by Vanson Bourne commissioned by Dell Technologies, "Global Data Protection Index 2021 Snapshot," carried out February – March, 2021. Results were derived from a total of 1,000 IT decision makers worldwide from both private and public organizations with 250+ employees.

IVASS : RICHIAMO AL RISPETTO DELLE MISURE RESTRITTIVE ADOTTATE DALLA UE IN RISPOSTA ALL'AGGRESSIONE MILITARE RUSSA IN UCRAINA

<https://www.ivass.it/media/comunicati/documenti/2022/ivcs538.pdf>



Roma, 7 marzo 2022

RICHIAMO AL RISPETTO DELLE MISURE RESTRITTIVE ADOTTATE DALLA UE IN RISPOSTA ALL'AGGRESSIONE MILITARE RUSSA IN UCRAINA

Banca d'Italia, CONSOB, IVASS e UIF richiamano l'attenzione dei soggetti vigilati sul pieno rispetto delle misure restrittive decise dall'Unione europea in risposta alla situazione in Ucraina.

Le misure sono consultabili sui siti della [pagina ufficiale dell'Unione europea](#), del [Comitato europeo dell'Unità di Informazione Finanziaria - UIF](#) e del [Comitato di Sicurezza Finanziaria](#).

Si ricorda che le misure – adottate dall'Unione europea mediante Regolamenti e Decisioni – sono vincolanti nella loro totalità e sono direttamente e immediatamente applicabili in ciascuno degli Stati Membri.

I soggetti vigilati sono tenuti, pertanto, a rispettarle, mettendo in atto i controlli e i dispositivi necessari, monitorando costantemente l'aggiornamento delle misure in questione.

Ai fini dell'adempimento degli obblighi di comunicazione delle misure di congelamento applicate ai soggetti designati andranno tenute altresì in considerazione le indicazioni fornite dalla UIF con il [Comunicato del 4 marzo 2022](#).

Nel contesto attuale, si raccomanda ai soggetti vigilati di esercitare la massima attenzione con riferimento al rischio di attacchi informatici, di intensificare le attività di monitoraggio e difesa in relazione a possibili attività di *espionage* e di adottare tutte le misure di mitigazione dei rischi che si rendano necessarie.

Si invitano, inoltre, i soggetti vigilati a considerare attentamente i piani di continuità aziendale (*business continuity plan*) e a garantire il corretto funzionamento e il pronto ripristino dei *backup*; in tale ambito, si sottolinea l'importanza di garantire la separazione dell'ambiente di *backup* da quello di esercizio, valutando la possibilità di prevedere soluzioni di *backup* offline (ovvia che non siano fisicamente o logicamente collegati alla rete) dei sistemi e dei dati essenziali.

Si invitano, infine, i soggetti vigilati a prestare attenzione nel continuo agli aggiornamenti forniti dal Computer Security Incident Response Team - Italia (cfr. <https://csirt.gov.it/comunicazioni/Ucraina>).

Si invitano, inoltre, i soggetti vigilati a considerare attentamente i piani di continuità aziendale (*business continuity plan*) e a garantire il corretto funzionamento e il pronto ripristino dei *backup*; **in tale ambito, si sottolinea l'importanza di garantire la separazione dell'ambiente di backup da quello di esercizio, valutando la possibilità di prevedere soluzioni di backup offline (ossia che non siano fisicamente o logicamente collegati alla rete) dei sistemi e dei dati essenziali.**

Broad spectrum of sophisticated cyber threats

Motivations, Techniques and Goals



Crime

Theft & extortion for financial gain



Insider

Trusted insiders steal or extort for personal, financial, & ideological reasons. Increasingly targeted because of privileged access to systems



Espionage

Corporate or Nation-state actors steal valuable data



Hacktivism

Advance political or social causes



Terrorism

Sabotage & destruction to instill fear



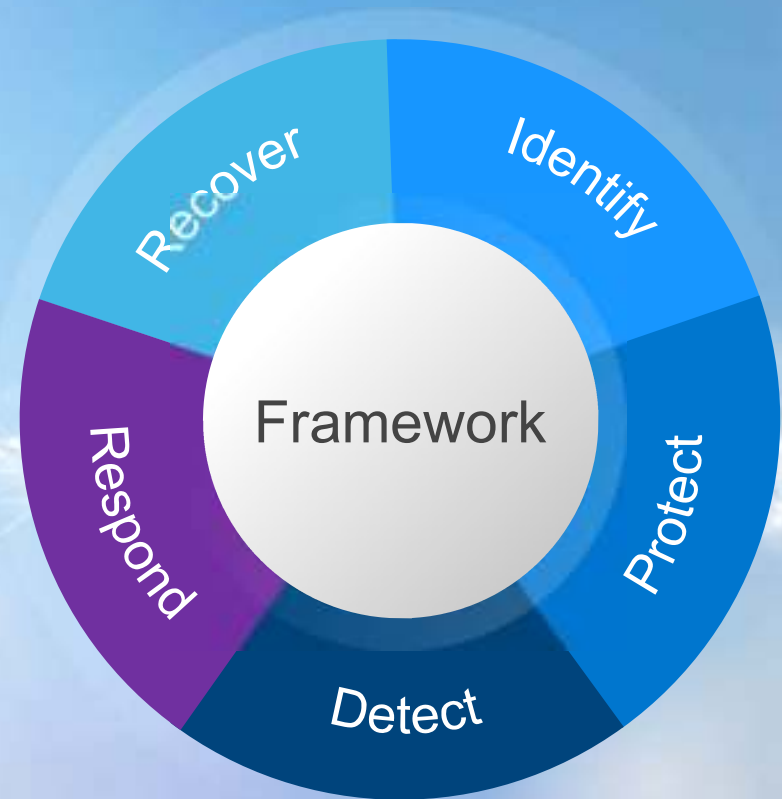
Warfare

Nation-state actors with destructive cyber weapons (NotPetya)

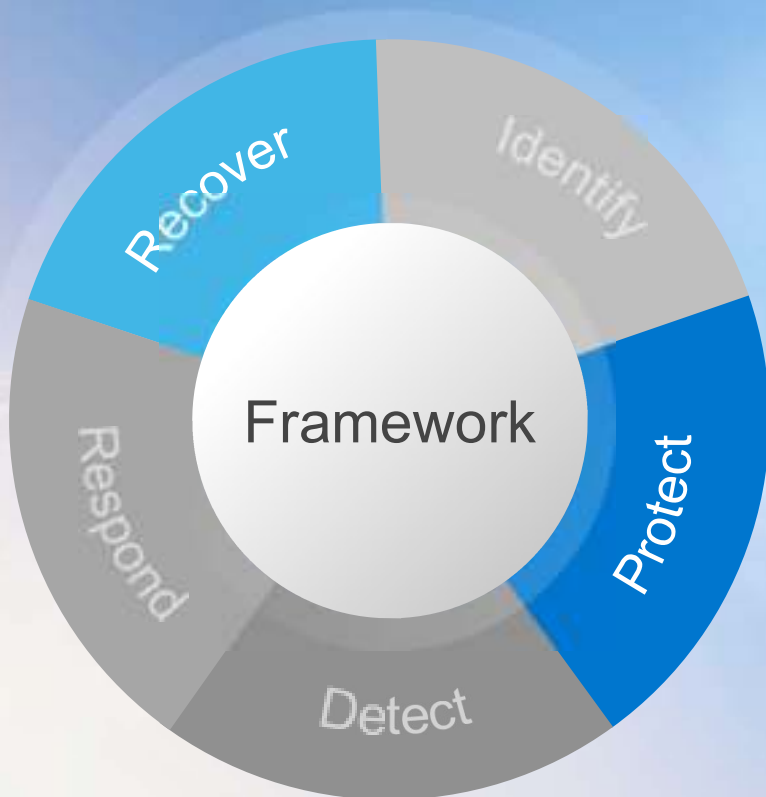
Cyber resilience is a strategy.

A high-level holistic strategy that includes cyber security standards, guidelines, people, business processes and technology solutions.

Example: [NIST Cybersecurity Framework](https://en.wikipedia.org/wiki/Cyber_resilience)



Cyber Recovery is a solution.



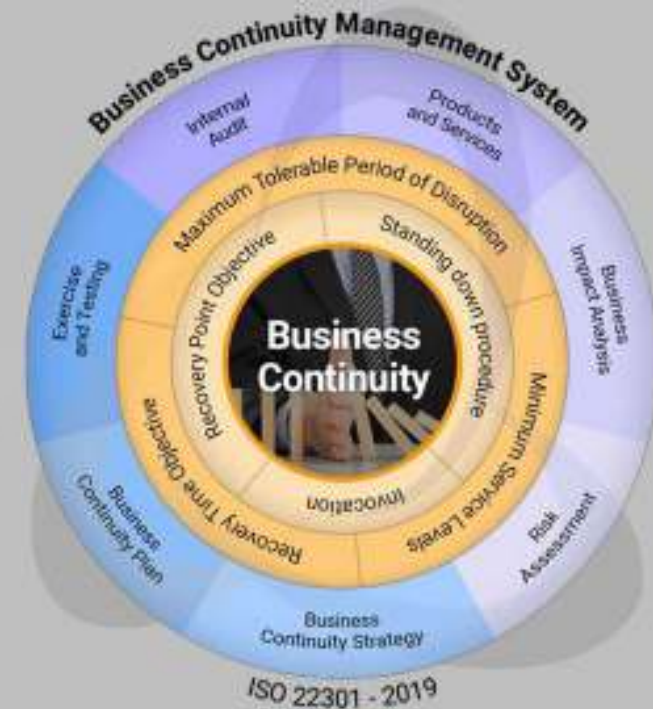
A data protection solution that isolates business-critical data away from attack surfaces.

Critical data is stored immutably in a hardened vault enabling recovery with assured data availability, integrity and confidentiality.

ISO 22301 – Cyber resilience come abilitatore

Molte aziende, anche a seguito della situazione COVID-19, si dichiarano ora maggiormente pronte ad implementare i principi di Business Continuity ed a conseguire la certificazione ISO 22301. Infatti, la certificazione risulta essere sempre più un parametro richiesto per essere conformi alle cogenti normative - soprattutto dopo l'avvento dell'Industria 4.0 – per partecipare a gare pubbliche e private, come dimostrazione della capacità di garantire la continuità nella fornitura di prodotti e servizi, nella supply chain e nella logistica a fronte di incidenti ed eventi avversi.

Come si evince nel “*The BCI Horizon Scan Report 2020*” sono molteplici i benefici derivanti dal conseguimento della certificazione ISO 22301 in termini di: aumento della **resilienza organizzativa**; continua misurazione e monitoraggio; **recupero più veloce a fronte di un'interruzione/incidente**; allineamento con gli altri operatori di settore; supporto agli stakeholder nella gestione dei rischi, miglioramento della customer satisfaction; migliore comunicazione e coinvolgimento del personale; leva per ridurre i premi assicurativi, etc



In a world where cyberattacks, data breaches and natural disasters can interrupt business continuity and quickly damage reputation, organisations and businesses need to implement, maintain and keep refining their **business continuity management system** (BCMS).

Disaster Recovery is not Cyber Recovery

Disaster Recovery / Business Continuity is not enough to address modern cyber threats

CATEGORY	DISASTER RECOVERY	CYBER RECOVERY
Recovery Time	Close to instant	Reliable & fast
Recovery Point	Ideally continuous	1 day average
Nature of Disaster	Flood, power outage, weather	Cyber attack, targeted
Impact of Disaster	Regional; typically contained	Global; spreads quickly
Topology	Connected, multiple targets	Isolated, in addition to DR
Data Volume	Comprehensive, all data	Selective, includes foundational services
Recovery	Standard DR (e.g., failback)	Iterative, selective recovery; part of CR

Cyber Recovery Requirements

Modern threats require modern solutions



The logo for Dell Technologies, featuring the word "DELL" in a stylized font where the 'E' is composed of three horizontal lines, followed by the word "Technologies" in a sans-serif font.

PowerProtect Cyber Recovery

Data Vaulting and Recovery Processes

