Digital Resilience: Managing Cyber-Security and Data Privacy

Dirk Vanderbist
EMBA Vlerick Business School

1 Content

2 The Need for Digital Resilience

Digital Resilience (DR) has become more important as our typical usage of digital systems has changed. The increased interconnection of systems to provide the same functionality compared to the previous monolithic systems architectures, made digital systems more complex. Other recent evolutions increased the complexity even more (Hodson, 2019; TIM-Review, 2015; Kaplan & Lung, 2018; Rothrock R. A., 2018b; Rothrock R. , 2018a):

- Client-Server models and Cloud computing moved systems outside the traditional control of organizations and distributed them across different interacting components.
- IoT moved intelligence and computing power to the edge of embedded devices.
- Big data massively increased the data volumes handled and stored by companies.
- Machine learning and artificial intelligence increase the complexity of business logic.
- Blockchain externalized key company data into externally controlled systems.
- Employee mobility took work outside the classical offices into the world of home, shared and ad-hoc offices. This connectiveness made work frictionless for the employee but also for the attacker.
- Increasing demands of end-user's data privacy and governance that went form fiduciary responsibly to regularity responsibilities (e.g. GDPR).
- The shift towards customer orientation moved systems away from systems of record to systems of engagement but also made that customer an important stakeholder to consider.

Because of these evolutions, IT technology deepened and widened its impact on strategic, tactical and operational company processes. It also meant that traditional rigid approaches to cybersecurity are not sufficient anymore. Traditionally cyber risk was managed through waterfall approaches comprises of rigid processes, with fixes sets of stages, milestones and deliverables (Hodson, 2019). A more

Table 2-1: Cyber Security vs. DR (Ayoub, Firth, & Nayaz, 2016)

Cyber Security	Digital Resilience
Disaster recovery – Retro-active – Continuous improvement	Threat prevention – Pro-active – Continuous innovation
External regulatory risk driven	Internal customer expectation driven
Manual detection and recovery processes	Automated detection and recovery processes
Disaster triggered discovery	Anomaly identification discovery
Legacy static monitoring	SMART system's monitoring
Internal knowledge bases for incident handling	Internal and external knowledge bases for incident handling

detailed comparison done by Ayoub et al can be found in (Table 2-1). A company's dependency on technology and connectivity increased, affecting the core business process and increasing the need of DR.

The changing world is sometimes not in line with the capabilities of companies (Ferdinand, 2015; UpGuard, 2019):

- Long development life cycles and technology refresh cycles due to technical debt and project backlogs.
- Critical infrastructure provided by a limited number of vendors resulting in vendor lock-in.
- Systems out-living people that worked on them or the infrastructure it was original designed for.

3 Evolving the Practice from Security to Resilience

Resilience can be defined as "the capacity of a system, enterprise, or a person to maintain its core purpose and integrity in the face of dramatically changed circumstances." (Rothrock R. , 2018a). Deriving a definition for DR for a company results in "assuring the continuation of the core processes when a company's digital systems are challenged by an adversary".

Traditionally companies approached DR in a fragmented and limited way with respect to the domain, the location and the scope (Crump, 2019). The domain of DR was restricted to the technical aspects of security and the direct effects on the organization of the break-down of these technologies. There was limited attention to the indirect impacts on the organization, although these might have a bigger strategic value e.g. reputation damage and client trust reduction. The activities of DR resided all within the ICT department instead of looking for the impact across all organizational functions. The scope of the activities was often retro-active solving issues and involved a static process in-stead of having a pro-active focus with a dynamic, to the circumstance, adaptive process.

First a traditional framework, i.e. the Cyber Resilience and Response model (CRR) from the Department of Homeland Security, will be looked into to explain some basic principles. Next the Business Continuity Management (BCM) framework will be used to highlight the core practices i.e. the cyber security framework from the National Institute of Standard and Technology (NIST). Finally, some additional practices that extend this framework to something more useful and adapted in the realm of DR, will be covered.

The CRR framework (Figure 3-1) has four phases – Prepare, Withstand, Recover and Adapt - as explained in Table 3-1 that apply different practices. CRR is a first level of resilience maturity focusing on being brilliant with the basics and demanding security by design.

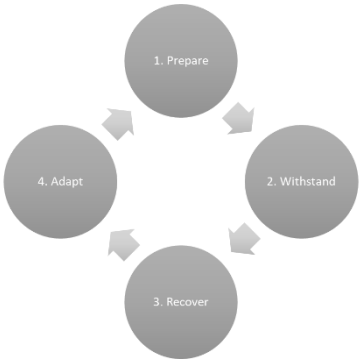

Figure 3-1: CRR framework (Analyst Exchange Program, 2018)

Table 3-1: CRR Practices – Adapted from (Analyst Exchange Program, 2018; Linkov & Kott, 2019; Engemann & Henderson, 2012; IT Goverance, 2020)

CRR Phase	*Resilience Feature* & "Phase Description"	Phase Applied Practices
Prepare	*Focused & Understood* "Predict and plan for threats and monitor critical functions for systems at risk"	• Put basic cyber hygiene in place: systems are patched and updated, access permissions enforce adequate authorization and authentication; and the data value is reduced for adversaries through hashing and encryption. • Train, exercise, validate and update response plans regularly.

		• Make systems agnostics and versatile to location, operator and technology used: loose coupling between system layers. • Demand security by design for systems: adopt DevSecOps principles to bake security in systems and have some minimal level of security assurance. • Safeguard data and systems against loss: back-up data, script & configuration and binaries.
Withstand	*Tolerance & Robustness* "Maintain business operations without performance degradation"	• Limit the damage by shutting down, isolating, containing and constraining affected resources and continue operating the non-affected resources and processes. • Coordinate and create a multi-layer of protection increasing the difficulty and cost for the adversary and the likelihood of detection; and diversify technologies used in the layers to reduce the likelihood of failure due to common resources. • Distribute critical assets across multiple systems to reduce the likelihood of a single point of failure for all critical processes or core assets; add redundancy in the system to avoid single points of failures in the system. • Restrict access of individual's privileges to operational need and put a segregation of duties model in place to avoid accumulation of privileges. • Diversify suppliers to reduce supply chain risks: remove single point of failures form the supply-chain when a supplier would be affected.
Recover	*Recoverable* "Rebound and restore to full operations, functions and performance"	• Restore environments and recover data from trusted sources and heighten protection during recovery.
Adapt	*Adaptive* "Perform change management to adjust existing plans based on experience from previous phases"	• Rearchitect systems and reorganize processes to reduce risk: redesign to reduce the dependencies of core processes on systems and data. • Model process for the possibility of being compromised. add un-happy path to handle affected systems in the process design next to the normal operation's happy path.

Next, the traditional NIST framework (NIST, 2018)(Figure 3-2) uses a 5-step approach - Identify, Protect, Detect, Respond and Recover. The activities from the framework are spread over three hierarchical levels i.e. incident executive level activities executed by the lead incident handler (LIH), management level activities executed by the executive in charge (EIC) and operational level activities worked on by incident response lead (IRL). NIST extends the CRR framework with business continuity and risk management elements as discussed in Table 3-2. NIST operates at the second level of resilience maturity where a data centric approach and a process centric approach is followed to classify, priority and mitigate risks.

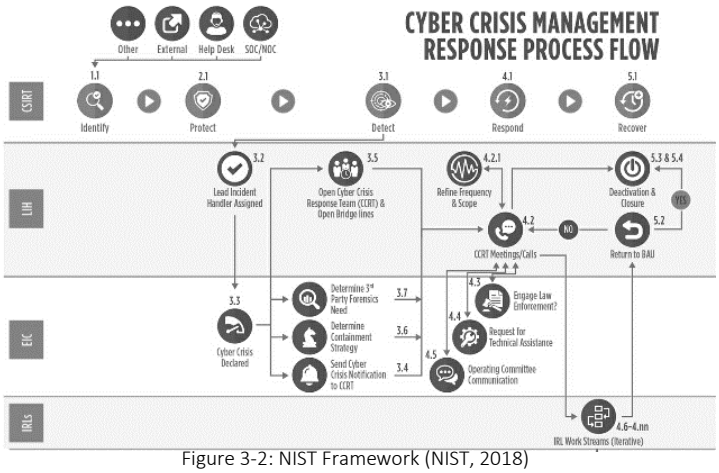

Figure 3-2: NIST Framework (NIST, 2018)

Table 3-2: NIST Practices – Adapted from (NIST, 2018; Engemann & Henderson, 2012; IT Goverance, 2020; Hodson, 2019; TIM-Review, 2015)

NIST Phase	Related CRR Phase	*Resilience Feature* & "Phase Description"	Phase Applied Practices (Additional to CRR)
Identify	-	*Objectified & Experienced* "Understand the cyber-security risk on systems, people, assets, data and capabilities"	• Perform a Business Impact Analysis (BIA) and a Risk Assessment (RA): assessing the critical organizational functions on cyber-related risks. • Create an incident priority model based on incident severity and impact: take into account different incident categories operational, financial, regulatory & legal and brand & reputation and prioritize efforts accordingly. • Organize C-suite awareness training: explain no system is impenetrable and it is not a question of if but of when. • Perform tabletop trainings: paper-based exercises to test the organization's decision making, response and recovery activities.
Protect	Prepare	*Planned & Controlled* "Limit or contain the impact of an incident"	• Establish objectives for business continuity and recovery (recovery time and point objectives). • Create and implement an Emergency Response Plan (ERP) and a Business Continuity Plan (BCP): define a strategy, create processes and identify roles and responsibilities (RACI). • Document and version control response and recovery plans: ensure access to most current plans by the response team. • Implement data retention policies: only persist data absolutely needed for business and the maximum time during which data is kept. • Segment systems according to business criticality: isolate business critical components from non-critical to limit propagation of incidents starting in non-critical systems. • Organize redundant site and equipment: private, guaranteed through mutual aid agreements or vendor-provided equipment (cloud computing).
Detect	Withstand	*Automated & Disclosed* "Discover a cyber-incident event"	• Automate tool responses: either an immediate action is taken or an event is flagged for investigation; gather and log forensic evidence. • Declare the incident: fulfill crisis notification requirements towards stakeholders and initiate crisis response.
Respond	Recover	*Collaborative* "Ability to contain the incident and to restore the impaired services or capabilities"	• Co-locate the crises response team in a war-room: centralize decision power and incident information. • Interact with the organization's environment: communicate with stakeholders, engage law enforcement, request technical assistance using pre-defined communication templates and scripts. • Execute a failover to non-affected infrastructure: a site failover to infrastructure in hot, warm or cold stand-by. • Restore in priority of business criticality: business critical operation first followed by non-business critical.
Recover	Adapt	*Adaptive* "Close the incident and return to Business as Usual"	• Update and maintain plans based on recent experience: ERP and BCP plans are evaluated on the validity of the assumptions, the executability of the plan and the achievability of objectives.

The final framework to look at, is the Adaptive Cyber Resilience framework (ACR). It adds yet another phase to the NIST model to come to a six-phase model – Anticipate, Identify, Protect, Detect, Respond and Recover (Figure 3-3) (Accenture, 2018). Besides the additional phase, ACR adds agility and adaptability to compensate for the rigidity of the other models and results in some additional practices summarized in Table 3-3. ACR operates on the third level of resilience maturity applying AI techniques to adapt processes and response real-time in a continuous way.

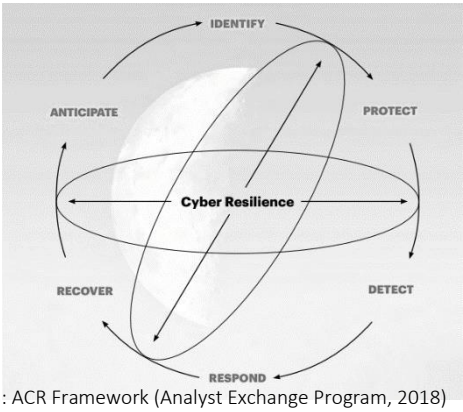

Figure 3-3: ACR Framework (Analyst Exchange Program, 2018)

Table 3-3: ACR Practices – Adapted from (Accenture, 2018; Hodson, 2019)

ACR Phase	*Resilience Feature* & "Phase Description"	Phase Applied Practices (Additional to NIST)
Anticipate	*Agility* "Anticipate and prepare for the unknown and unforeseen"	• Determine user profiles: a user profile contains normal usage and behavior in relation with systems and processes. The profile is not one time fixed but adaptive during the user's life time (tactical adaptation). • Expect the adversary to adapt: update procedures and technology frequently to avoid complacency.
Protect	*Planned & Controlled* "Limit or contain impact of an incident"	• Support situation awareness: enhance understanding of threats by gathering information on patterns and trends in adversary behavior (operational adaptation) and from general research (tactical adaptation). • Make random and unpredictable system changes: increases uncertainty thus making it more difficult for the adversary (software defined networking). • Deceive adversary so he reveals his presence or loses time: trap adversary by presenting fake systems or data to persuade them going after this (honey-pots; sand-boxes). • Execute offensive and defensive testing: exploratory testing to check if creative new angles of attack would result in new threats (red and blue testing).
Detect	*Automated & Disclosed* "Discover a cyber-incident event"	• Monitor for abnormal user behavior: behavior not in line with the user profile should be flagged for investigation; anomaly detection (User Behavior Analysis). • Continuous validation of correctness of data: pro-actively identify incremental changes that can, combined, lead-up to an incident to avoid adversaries creeping up.

4 Benefits and Costs of Digital Resilience

Most of the time a topic will reach C-levels attention once it potentially could affect the bottom line and objectives of a company, which is the case for cyber incidents. Becoming DR is a long-term process since it involves the full organization in bread and depth (Williams & Manheke, 2010) referring to the different practices discussed in the paragraph 4. The benefits are harder to quantify and are expressed as minimizing the cost related to direct and indirect effects (Table 4-1) of a cyber incident this by preventing or reducing exposure and the related mitigation costs. Some of these effects are intangible like trust and confidence.

Cyber risk, like any other risk, can be handled mitigated in four different ways (Kaplan & Lung, 2018; Rothrock R. , 2018a; Engemann & Henderson, 2012): avoidance (eliminate the risk), transfer (transfer the effects to another party), reduction (reduce the effects) and acceptance (endure the effects). It is clear that avoidance and acceptance are not viable options since the current environment makes it impossible to eradicate cyber risk and stakeholders will not allow you to ignore. The reduction option is what DR is aiming at. Transfer can be obtained by mitigating the risk through insurance policies. Insurance often only addresses the direct, out-of-the-pocket, costs and is less helpful to resolve to organizational issues beyond reducing the financial damages: revenue loss, legal indemnification costs and stock-market value loss.

Table 4-1: Cyber Incident Effects – Adapted from (Engemann & Henderson, 2012)

Cyber Incident Effects
Direct Effects • Destruction of assets • Loss of revenue and business opportunities • Reduced competitive capabilities
Indirect Effects • Decreased customer satisfaction • Decreased investor confidence • Damage of reputation and brand • Adverse media coverage • Legal exposure • Missed reporting deadlines • Increased risk rating • Increased insurance premium

The benefits of Cyber Resilience (CR) are avoiding the direct and indirect effects of cyber incidents, by preference, in a pro-active way (Clarke & Knake, 2012). The cost related to CR are enumerated in Table 4-2. There are some trade-offs to be made between cyber-resilience and operational performance. In reducing the cyber risk components are added to the IT landscape and activities to the business processes i.e. additional technical layers, redundant components, monitoring, and logging. These have a negative effect on the systems performance. To be cost-effective CR solutions must scale to avoid increasing systems' scope would more than proportionally increase the CR costs (Hodson, 2019). This is achieved through automation, self-correcting and adapting practices as explained in the ACR framework in paragraph 4.

Table 4-2: Cyber Incident Costs – Adapted from (Engemann & Henderson, 2012)

Cyber Resilience Costs
• Analyzing, defining, updating and maintaining the company's as-is and to-be Cyber Resilient state. • Execution of Cyber Resilience improvement plan to implement the cyber practices. • Investment in assets for monitoring, protecting, safeguarding, redundancy and response. • Dedicated human resources involved in Cyber Resilience activities. • Executing training and awareness programs. • Insurance costs for transferred cyber risks. • Resilience vs. Performance trade-offs.

5 Measuring Digital Resilience

The maturity of DR can be measured using metrics at strategic, tactical and operational level (BIS, 2018) in the organization (Table 5-1). At strategic level it is checked how much DR receives C-level attention. The tactical level measures the capabilities against best practices of DR and finally the operational level looks at the effectiveness and efficiency of DR.

Table 5-1: DR Maturity Metrics – Adapted from (BIS, 2018)

Topic	Metric	Maturity Measure
Strategic		
Governance	Budget allocated: % budget / CAPEX % budget / OPEX	An appropriate amount of the company's budget is allocated to develop, implement and maintain DR activities. DR maturity is measured by comparing the available budget to a benchmark budget for the required level.
Priorities	Relative order: weighted average priority	An appropriate level of attention of the company in its strategic objectives is given to DR activities. DR maturity is measured by the

		weighted average order of DR activities: i.e. priority number and proportion of DR vs non-DR objectives.
Tactical		
Staffing	Resources: % attrition DR staff % trained / DR staff	An appropriated level of staff involved in the DR activities, is experienced and trained. DR maturity is measured by attrition rate of the DR staff (low means high DR maturity) and percentage of people with an DR identified role that is strained (high means high DR maturity).
Scaling	Costs & Performance: % cost increase / # business processes % throughput time / average process duration	An appropriated scaling potential is required. DR maturity is measured in a less than proportional costs increase and process throughput time increase for an increased number of business process executions. More than proportional increase indicates a high level of manual or semi-automated DR practices.
Practices	Applied practices: % applied / total practices	An appropriated number of DR practices are in place. DR maturity is measured by the amount of implemented practices compared to the set of available best practices (see CRR, NIST and ACR frameworks in paragraph 3).
Trust	Tests: % test success / total tests	An appropriate test success level must be achieved during penetration, ethical hacking, discovery and treat DB recognition testing. DR maturity is measured by the number of successful tests compared to the total number of tests. A high number means a trust wordy robust system or high DR maturity.
Operational		
Processes	Process focus: % recovery / total % preventive / total % adaptive / total	An appropriate number of the DR processes is related to more advanced practices. DR maturity is measured by the percentage of implemented recovery (low DR), preventive (medium DR) and adaptive (high DR) practices.
Incidents	Stop location: % notified / total % recovered / total % prevented / total % predicted / total	An appropriated number of incidents is detected at the correct location. DR maturity is measure by the percentage of incidents detected at a specific location: notified (i.e. externally detected, DR maturity none), recovered (low), prevented (medium), predicted (high).
Efficiency	Recovery time and point: % downtime / uptime % unrecovered data / stored data % exposed data / stored data	A minimal downtime and maximum amount of data recovered. DR maturity is measured as relative recovery speed, lost data and exposed data.

6 What is still Missing?

In paragraph 4, whilst discussing the benefits, a trade-off between DR and company performance was identified. This was a trade-off between the potential costs of an incident and the impact of DR on the cost performance and business process performance. The trade-off analysis can lead up to some perverse effects. Imagine if an insurance would cover the direct and indirect effects of cyber incidents, this might result in a

company not caring about the impact of such an incident on stakeholders (Williams & Manheke, 2010). Luckily some regulatory initiatives, like GDPR, have forced company to internalize these effects. For the areas were this is still not the case, Corporate Responsibility and Sustainability should incorporate a cyber responsibility aspect to avoid an insurance greenwashing effect.

Measuring DR was the topic of paragraph 5. The biggest challenge is quantifying some of the DR aspects. The DR practices, cf. paragraph 3, talk about the need of testing and training DR capabilities. This can be problematic for a company as a test might result in a real disaster or might require the test object to be destroyed (e.g. how to test a cut optical fiber might require effectively cutting the wire). The same applies for ethical hacking techniques that might result in real business disruptions. This is a risk, i.e. triggering an adverse effect, vs trust, i.e. measuring the level of DR, trade-off.

Finally, companies have what is called a risk-appetite. This is a risk vs. cost and benefit trade-off, were a company can gain more by accepting more risk. But when things go sour the losses will be more substantial as well. The trade-off will be settled by the level of risk-adverseness of the industry the company is active in and the shareholders expectations.

7 References

7.1 List of Figures

7.2 List of Tables

7.3 Bibliography

Accenture. (2018). *The Nature of Effective Defense: Shifting from Cybersecurity to Cyber Resilience.* Chicago: Accenture Dederal Services.

Analyst Exchange Program. (2018). *Cyber Resilience and Response.* Washington: Department of Homeland Security.

Ayoub, R., Firth, C. M., & Nayaz, M. (2016). *Cyber Resilience in the Digital Age.* EY.

BIS. (2018). *Cyber-Resilience: Range of Practices.* BIS.

Clarke, R. A., & Knake, R. K. (2012). *Cyber War: The Next Treat to National Security and What to Do About It.* New York: Harper Collins Publishers.

Crump, J. D. (2019). *Cyber Crisis Management Planning: How to reduce cyber risk and increase organizational resilience.* Jeffrey Crump.

Engemann, K. J., & Henderson, D. M. (2012). *Business Continuity and Risk Management.* Brookfield: Rothstein Associates.

Ferdinand, J. (2015). Building organisational cyber resilience: a strategic knowledge-based view of cyber security management. *Journal f Business Continuity & Emergency Planning, 9*(2), 185-195.

Garista, P., & Pocetta, G. (2014). Digital Resilience: meanings, epistemologies and methodologies for lifelong learning. *INDIRE Roma* (pp. 1-4). Roma: INDIRE.

Garside, D. (2018, August 1). *Digital resilience – a step up from cybersecurity.* Retrieved from CSO: https://www.csoonline.com/article/3293898/digital-resilience-a-step-up-from-cybersecurity.html

Hodson, C. J. (2019). *Cyber Risk Management: Prioritize Threats, Identify Vulnerabilities and Apply Controls.* New York: Kogan Page.

IT Goverance. (2020, April 22). *Cyber Resilience*. Retrieved from IT Governance: https://www.itgovernance.eu/nl-be/cyber-resilience-be

Kaplan, J., & Lung, H. (2018, June 20). *igital resilience: Seven practices in cybersecurity.* Retrieved from McKinsey Digital: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-blog/digital-resilience-seven-practices-in-cybersecurity

Kharchenko, V. S. (2017). *Secure and Resilient Computing for Industry and Human Domains.* Kharkiv: Kharkiv Aviation Institute.

Linkov, I., & Kott, A. (2019). *Cyber Resilience of Systems and Networks.* New York: Springer.

Martin, C., & Samans, R. (2018). *Cyber Resilience: Playbook for Public-Private Collaboration.* Boston: World Economic Forum.

NIST. (2018, April 16). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Petrenko, S. A., & Vorobieve, D. E. (2019). Method of Ensuring Cyber Resilience of Digital Platforms Based on Catastrophe Theory. *SCMI* (pp. 1-19). St. Petersburg: IEEE.

Rothrock, R. (2018a). *Digital Resilience: Is Your Company Ready for the Next Cyber Threat?* New York: American Management Association.

Rothrock, R. A. (2018b, September 3). *Five Tips For Building Digital Resilience Into Your Business Plan.* Retrieved from Chief Executive: https://chiefexecutive.net/five-tips-for-building-digital-resilience-into-your-business-plan/

TIM-Review. (2015). Cyber-Resilience in Supply Chain. *Technology Innovation Management Review* (pp. 1-46). Carleton: Carleton University.

UpGuard. (2019, November 20). *What is Digital Resilience?* Retrieved from UpGuard: https://www.upguard.com/blog/what-is-digital-resilience

Williams, P. A., & Manheke, J. R. (2010). Small Business - A Cyber Resilience Vulnerability. *International Cyber Resilience conference* (pp. 112-119). Perth: Cyber Resilience conference.