Deloitte.

Cybersecurity Architecture Risks

Is your business prepared for a global system outage?

Executive summary

As organizations continue to digitize, automate, and adopt cloud technologies, they further increase their dependency on security vendors to support and run their critical security and business processes. In the event of a global information technology (IT) outage, critical services that support economic stability and public safety can be severely disrupted. In many cases, these services include critical sectors such as transportation, health care, government services, and telecommunications among others. These disruptive events highlight the need for organizations to consider widespread IT outages when building their security architecture, mapping IT dependencies to critical business processes, updating incident response and disaster recovery plans, and refreshing third-party risk management strategies.

It is widely understood that an IT outage is distinct from a cybersecurity incident. However, an outage can create vulnerabilities in an organization's security posture when critical security tools (e.g., endpoint detection and response (EDR), antivirus, firewalls) become unavailable. Such impacts can disable essential security solutions for monitoring critical data and processes, potentially affecting availability. This availability, a vital component of the CIA triad (Confidentiality, Integrity, Availability), facilitates timely and reliable access to and use of information or processes.

While an IT outage primarily affects system availability, it also introduces security risks that can impact critical business processes across the entire CIA triad. These risks emerge when opportunistic cybercriminals exploit IT outages to launch attacks, posing risks to confidentiality (preserving authorized restrictions on information access and disclosure) and integrity (guarding against improper information modification or destruction). Cybercriminals exploit the uncertainty in situational awareness when an IT outage disrupts monitoring and protection controls. This uncertainty is particularly evident when cybercriminals exploit the shift in focus when IT and security teams are initially trying to understand the cause of an outage, which increases the success rate of cybercriminal exploitation methods.

The approach to refreshing an organization’s cybersecurity architecture, technology stack, and processes while managing its risk tolerance is a multi-faceted challenge. This whitepaper presents strategies and leading practices to consider for enhancing your cybersecurity posture and reducing the potential impact of a broad IT outage. Among the strategies, organizations can consider following leading practices that support the CIA triad, including Zero Trust architecture, defense-in-depth strategies, least privilege, network segmentation, strong identity and access management and privilege access management controls, and mature training and awareness programs.

Key actions:

- **Map system dependencies to mission objectives:** It is important to inventory and map system dependencies to critical assets that support fulfilling mission objectives. This is crucial in understanding the business risks during an outage.
- **Include IT risk scenarios in response and recovery plans**: Selecting a security architecture approach calls for accepting a certain level of risk and recognizing that IT outages are an unavoidable reality, especially when implementing redundant systems is not feasible. Therefore, prioritizing mature incident response (IR) and disaster recovery (DR) plans, along with regular tabletop exercises (TTXs), are essential to providing a quicker response and recovery for organizational resiliency.
- **Understand that resiliency is not confined to a single discipline**: Organizational resiliency is not limited to redundancy but incorporates multiple strategies, including response, restoration, recovery, and reorganization.
- **Embed tiering across third parties**: When managing third parties, it is crucial to incorporate tiering into the third-party risk management process. This puts focus on services that are more critical and pose higher risks to the business receive greater rigor and scrutiny.
- **Approach third-party contracts with a resilience mindset**: Organizations should review and strengthen their contractual agreements. This may include stipulations for advanced notifications before rollouts and the establishment of controlled rollouts that allow the organization to revert to previous versions if issues arise.

Assessment of the current landscape

How can a business process be recovered without an understanding of the supporting systems?

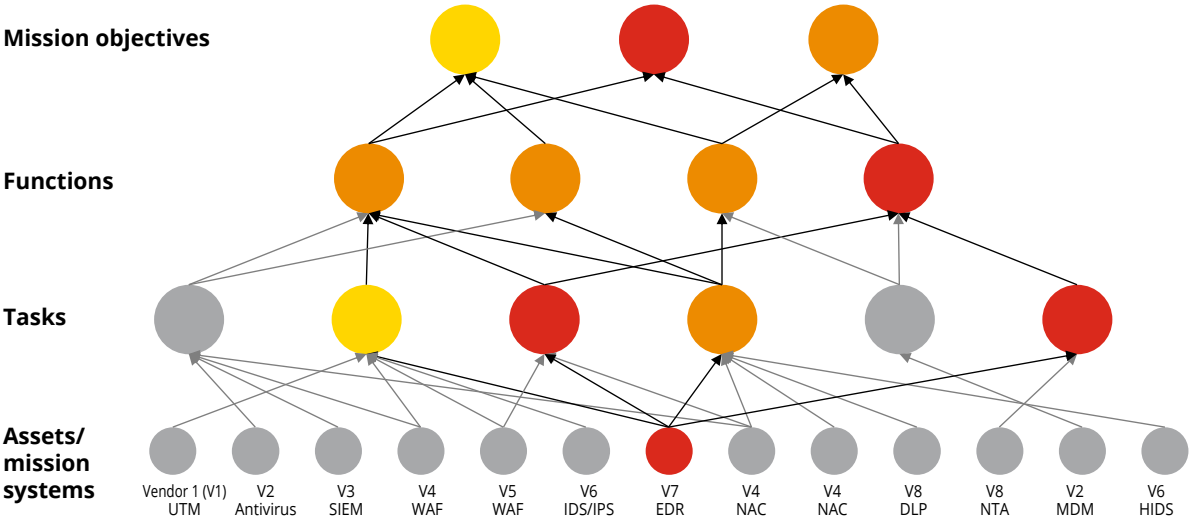
Organizations should conduct a broad risk assessment to identify their critical assets and the dependencies of those assets. Many organizations face challenges with maintaining an asset inventory, including inventorying their software and determining its location within the environment. Having a thorough inventory is important for mapping system dependencies to mission-critical objectives (see Figure 1). Organizations should evaluate how an IT outage may impact the availability of essential cybersecurity solutions. Understanding this impact is vital, as it increases security risks due to the absence of monitoring and protection, which can lead to significant operational consequences for the business.

According to recent Gartner® research, "By 2026, **60%** of cybersecurity functions will implement business-impact-focused risk assessment methods, aligning cybersecurity strategies with organizational objectives"[2]

Do your incident response and disaster recovery strategies incorporate scenarios of real-world IT failures?

In an era where digital infrastructure forms the backbone of business operations, an organization's resilience hinges on its ability to swiftly and effectively respond to IT outages, which are commonly caused by cyberattacks, hardware failures, software bugs, and natural disasters. As detailed further in this paper, selecting a security architecture approach necessitates a degree of risk acceptance. Therefore, organizations should proactively prepare for IT

Figure 1: Mapping system dependencies to business decomposition tiers[1]



UTM = Unified Threat Management
SIEM = Security Incident and Event Management
WAF = Web Application Firewall
IDS/IPS = Intrusion Detection System/Intrusion Prevention System
EDR = Endpoint Detection and Response
NAC = Network Access Control
DLP = Data Loss Prevention
NTA = Network Traffic Analysis
MDM = Mobile Device Management
HIDS = Host-Based Intrusion Detection System

outages by not only focusing on redundant systems which can still result in an outage, but also developing comprehensive IR and DR plans with a strong IT focus.

One of the most challenging aspects of a crisis is often determining the appropriate points of contact. Therefore, it is essential to document internal communication protocols. Additionally, navigating external communications can be complex but equally important. This includes coordination with third-party vendors, incident response retainers, cyber insurance providers, external legal counsel, law enforcement agencies (both local and federal), public relations firms, and other relevant entities. Ensuring these details are thoroughly documented within IR and DR plans is important for a streamlined and effective response.

Documenting IR and DR plans is merely the first step; the actual test of their efficacy is frequent and rigorous testing. TTXs are a leading practice for evaluating the readiness and relevance of these plans. Through TTXs, organizations can pinpoint the specific needs and roles at each stage of the response process, fostering a collaborative mentality essential for efficient orchestration. Mature TTXs incorporate IT and Operational Technology (OT) teams, encouraging collaboration and integrating diverse processes and tools. By involving these broader teams, organizations gain varied perspectives and can enhance their preparedness for various scenarios, including IT outages. This broad approach means each facet of the organization is aligned and ready to respond accordingly.

Increasing reliance on vendors necessitates tighter contract commitments and third-party risk management (TPRM) strategies

When managing third parties, it is essential to embed tiering across the TPRM process to ensure more rigor and scrutiny are applied to services that are more critical and present a higher risk to the business. Organizations can leverage system dependency maps or business capability models to understand and assign vendor tiers based on a systems-level of criticality to business operations. A prerequisite for embedding tiers for third parties involves meeting industry-standard controls, notably establishing a broad software asset inventory and understanding where that software lives in the environment, which is a leading practice outlined in the Center for Internet Security's (CIS) critical security controls.[3]

> The Gartner Press Release reveals that "Despite increased investments in third-party cybersecurity risk management (TPCRM) over the last two years, **45%** of organizations experienced third party-related business interruptions."[4]

Furthermore, Deloitte has observed that many organizations lack internal controls mandating regression testing. This testing is important to make sure that updates, configuration changes, or patches do not negatively impact existing system functionality before deployment. While automatic updates are designed to enhance system performance, they can introduce risks that may disrupt critical services. Therefore, organizations should review and strengthen their contractual agreements. This may include stipulations for advanced notifications before rollouts and the establishment of controlled rollouts that allow the organization to revert to previous versions if issues arise.

Another critical component of TPRM strategies involves actively testing business continuity and DR plans with necessary third parties. Often, organizations limit their efforts to auditing policies to ensure testing is outlined, thereby missing an opportunity to actively test these plans with their critical material service providers, which should not only be contractually written but tested through performance. This oversight can lead to a false sense of security, delayed response times, and a lack of risk awareness at the team level. Ultimately, inadequate testing increases the likelihood of extended downtimes.

The benefit of testing extends to the IT, OT, and cybersecurity professionals at the team level, who are responsible for executing the recovery and business continuity plans. This ensures that response teams are familiar with their material service providers, know who to contact during an outage, and understand what to prioritize based on system dependencies mapped to critical services.

Risk reduction strategies

Redundancy may not be the answer to resiliency

Resiliency refers to an entity's ability to withstand disruptive events while maintaining its core functions. Deloitte has observed some clients who believe resiliency is limited to redundancy or backups. However, Deloitte promotes the concept that resiliency is not confined to a single discipline but incorporates multiple strategies, including response, restoration and recovery, and reorganization. Organizations should establish resilience design standards and fully embed them throughout the organization, including within the extended enterprise of third parties and suppliers.

Unlike small to medium-sized organizations, larger organizations with potentially higher budgets can more easily consider redundant systems that map to critical processes. These systems can support a failover mechanism to maintain continuity of security operations during an IT outage and support resiliency. However, in some cases, redundancy is not a practical solution and certainly not a holistic approach to resiliency.

In security architecture, redundancy alone is not the optimal approach for resiliency. For instance, engineering teams recognize that for some security solutions, redundancy may not be practical. This is because some security solutions often do not integrate well with each other, as exemplified by the incompatibility of deploying two EDR solutions simultaneously at the kernel level.

Deloitte has observed that some organizations have displayed the ability to recover quickly from an IT outage by rolling back channel files after receiving a flawed update. These measures have historically enabled clients to recover effectively within a few hours. However, in other instances, some organizations spend weeks struggling to recover, which is commonly influenced by a lack of understanding of system dependencies and preparedness from a process perspective.

To maintain resilience in the face of an IT outage that disrupts operational and security functions, organizations should consider not only redundancy and failover mechanisms but also incorporate fault tolerance where a level of risk acceptance is required (e.g., when redundant systems are not a practical solution). This involves focusing on maturing existing processes across IR, DR, and TPRM, along with communication and coordination of TTX that incorporate IT outage scenarios. Organizations can also focus on tightening vendor contracts to ensure updates are incrementally rolled out to systems. This is particularly critical in cloud and software-as-a-service (SaaS) environments, where vendors are responsible for maintaining the underlying platform. These processes and due diligence measures are essential as organizations increasingly rely on vendors to support their enterprise security architecture.

How do current trends in enterprise security architecture mitigate or exacerbate the risks of a global IT outage?

A robust enterprise security architecture is essential to safeguarding the CIA of critical assets and business processes. Therefore, organizations must evaluate how trends in security architecture might mitigate or exacerbate the risks associated with a global IT outage that involves the loss of availability across security solutions.

Many organizations are trending toward "platformization" through a Platform Play security architecture design compared to the Best of Breed approach.[5] Platform Play refers to a unified, integrated security framework consolidating various security functions and tools into a single, cohesive platform. Organizations that adopt the Best of Breed approach typically select multiple tools from various vendors, rather than opting for a comprehensive suite of tools from a single, well-known brand that offers integrated solutions. Without delving too deep into the intricacies of the two methods, Figure 2 illustrates that both approaches have benefits and drawbacks that organizations need to consider when implementing their preferred approach.

When considering how current trends in enterprise security architecture mitigate or exacerbate the risks of a global IT outage, it is essential to evaluate these two industry-recognized approaches: the Platform Play approach (e.g., vendor ecosystem) and the Best of Breed approach (e.g., vendor diversification).

Figure 2: Deloitte's perspective on the two security architecture approaches

Best of Breed

Benefits

- Provides a leading marketplace solution for individual cybersecurity capabilities (e.g., SIEM, EDR, Cloud Security)
- Enables customization and in-house engineering to improve capabilities and satisfy requirements
- Promotes an iterative approach to security operations that changes as capabilities and technology improve
- Mitigates the impact to cybersecurity risk posture associated with making architectural changes

Drawbacks

- Requires complex, and sometimes unproven, engineering efforts
- Multiple vendors involved in troubleshooting or vendors unable to assist with troubleshooting issues
- Distributes vendor contracting and removes economies of scale from pricing
- Requires in-house security operations teams to be involved in training and designing operational guidance

Platform Play

Benefits

- Reduces the need for complex engineering and maintenance effort due to out of box unified integrations and correlations
- Provides recommendations for how to achieve specific outcomes, training for all security capabilities, and reduces redundant capabilities
- Reduces long term overall cost with platform bundling and economies of scale
- Directs accountability to vendor for all troubleshooting all issues within the stack

Drawbacks

- Products within a platform may relatively underperform and may need time to meet requirements
- Limits customization opportunities to improve capabilities or meet unfulfilled requirements
- Reduces flexibility to adopt new security capabilities in the future due to platform limitations and vendor lock-in
- Impacts costs and risk posture during transition while potentially increasing time-to-value (TTV)

Whether an organization adopts a Platform Play or a Best of Breed approach, reliance on a single vendor's security solution or integrating multiple technologies can both lead to an IT outage.

However, the Platform Play approach can offer certain advantages in terms of having a single point of contact during such incidents. This can streamline incident response and disaster recovery efforts, as a single vendor with in-depth knowledge of the organization's environment can reduce complexity. Paradoxically, a single point of contact further increases the need for tighter contracts and testing, especially considering the implications if a vendor's support does not meet expected standards. Additionally, organizations should consider the importance of vendor transparency, such as understanding upstream services or fourth-party dependencies to assess associated risks. Vendor transparency is generally more manageable when working with a single vendor, as opposed to navigating the complexities of multiple vendors, which can complicate risk identification for fourth-party dependencies in a Best of Breed approach.

Ultimately, organizations should conduct a thorough cost-benefit analysis and risk-based analysis to determine which approach aligns best with their specific needs, including:

- **Interoperability of redundant tools**: Assessing the compatibility and integration of multiple security tools from different vendors.
- **Cost to operationalize multiple vendor products**: Evaluating the financial and resource implications of managing and maintaining products from various vendors.
- **Ability to train and maintain an engineering team**: Identify the difference in training requirements among the two approaches: Best of Breed involves a highly skilled engineering team capable of managing and integrating diverse tools and solutions. In contrast, a Platform Play may require less specialized training as the platform provider handles much of the complexity.
- **Operational efficiencies aligned with risk tolerance**: Consider the potential efficiencies or inefficiencies introduced by multiple vendor solutions and analyze the organization's risk appetite where specific approaches may require stringent oversight while providing tailored solutions.
- **Assessment of diversification benefits**: Determine whether the organization genuinely benefits from additional protection through redundant solutions or vendors. This may not always be the case, as highlighted by the incompatibility of deploying two EDR solutions.

Organizations will need to acknowledge and manage a certain level of risk while conducting this cost-benefit analysis. The goal is to strike a balance between the potential benefits of vendor diversification and the ecosystem-platform model and the operational complexities they may introduce. This means that the chosen security architecture approach provides robust protection without unnecessary redundancy, in which the cost outweighs the benefit. By incorporating a risk-based approach alongside the cost-benefit analysis, organizations can prioritize their investments in cybersecurity measures that address the most significant risks, thereby achieving a balanced strategy that maximizes both financial and security outcomes.

Future trends and emerging technologies

Operational resiliency is a top priority for regulatory authorities

Third-party service disruptions can have significant financial, operational, and reputational consequences. Most notably, the consequences of operational disruptions that increase national security risks. The Financial Services Industry (FSI) is an example of how regulators across the industry are enforcing operational resilience requirements in a forward-looking manner to prevent harm before it occurs. Organizations can learn from FSI what to expect if operational resiliency is no longer a choice but a requirement.

FSI regulators have taken measures to require safeguards for operational resiliency to defend critical financial services. The Basel Committee on Banking Supervision (BCBS) published the Principles for Operational Resilience (POR) in 2021, which aims to strengthen the ability of banks to "withstand operational risk-related events that could cause significant operational failures or wide-scale disruptions in financial markets."[6] Since then, regulations have come into force from many global authorities, including the Australian Prudential Regulation Authority[7], the European Commission[8], the Financial Conduct Authority[9], the Hong Kong Monetary Authority[10], the Monetary Authority of Singapore[11], and others, which are testing the resilience of global financial institutions. The requirements across various regulations include identifying critical business services, setting impact tolerances for critical services, performing mapping and testing to ensure they remain within impact tolerances, scenario testing, incident management, classification, reporting, and mapping dependencies and resources to those critical services.

Regulatory requirements for operational resiliency enforced on the FSI serve multiple purposes, including maintaining the reliability and availability of financial services for consumers and maintaining the stability of financial markets. Other industries can learn from FSI's proactive approach, particularly those in critical sectors such as energy and utilities to provide essential services and aerospace and health care sectors, which bear the responsibility

of safeguarding human lives. Widespread system outages can result in the disruption of patient care and flight management systems. While organizations cannot plan for every possible scenario, they can implement measures to prepare for events, incorporating risks related to IT outages that disrupt security operations and business functions. Based on historical evidence, as regulators focus on cyber and IT impacts on national security, it is possible for operational resiliency requirements to be enforced across industries. This is particularly relevant for publicly traded companies, many of which support critical infrastructure and services.

Emerging technologies can embed insights into your supply network operations

Global supply networks have never been more complex and are increasingly subject to disruption. Emerging TPRM tools can integrate thousands of relevant data sources, leveraging technology such as artificial intelligence (AI) and machine learning (ML), to deliver next-generation insights embedded into an organization's end-to-end operations. Emerging TPRM tools provide greater intelligence on potential impacts and broader business implications to help organizations anticipate, avoid, and respond to potential disruptions.

Emerging TPRM tools can provide business risk assessments related to an IT outage, identifying how it affects critical services. For example, organizations can leverage emerging TPRM tools to perform risk assessments around cybersecurity posture related to vulnerabilities and threats and address risks related to vendor diversification or a lack thereof. These tools include a supplier discovery engine, data ecosystem, near real-time alerts (e.g., disruption/status), advanced company search, supplier dashboards, advanced link analysis, interactive dashboard, case/collaboration workflow, and cloud hosting. These TPRM tools are designed to support:

- **Improved network visibility**: Establish deeper network visibility and supply chain mapping with site locations while understanding risks from a geographic perspective related to natural disasters.
- **Better sensing of signals:** Sense risks and receive near real-time proactive alerts with scheduled event monitoring and network analytics.
- **Greater operational efficiency**: Use advanced network insights to help drive cost optimization, structural improvements, and near-term risk mitigation; act faster than the competition; address margin erosion (lost sales, increased input costs due to disruption); maintain customer service levels; and enhance brand trust (shipping times, product availability).
- **A centralized platform and a single source of truth**: Leverage flexible data source integration and network illumination powered by AI.

Final thoughts

Is your organization addressing potential IT outage risks?

Defending a complex security environment, increasingly dependent on IT vendors to safeguard mission-critical operations, is a complex task. Adopting a mindset that acknowledges incidents will happen can help organizations as they adopt effective approaches for maintaining a proactive security posture. It is important that organizations have a deep understanding of the technology in use and that it is designed and operated with resilience in mind. This involves configuring systems aggressively—implementing security and operational settings that prioritize enterprise-wide protection and performance—while maintaining a balance between value and risk. Second, organizations should prioritize developing and maintaining strong relationships, both externally and internally. Externally, this involves cultivating connections with technology suppliers and third-party vendors to ensure that the right contacts are readily available in case of issues. Internally, it is essential to foster a unified approach where engineering and operations teams work seamlessly together, promoting regular collaboration to enhance overall efficiency and resilience. Third, develop and test IT and security contingency plans, exercising them at all levels, from technical teams to the C-suite. It is critical that executive sponsorship takes a leading role, and it should be evident throughout all resilience activities. Executive sponsorship should support strategic alignment, ensuring all resilience activities align with the organization's mission objectives and risk appetite.

References

1. Staff, "Crown Jewel Analysis," n.d. [Online]. Available: https://www.safie.hq.af.mil/Portals/78/documents/IEE/Energy/CJA_2021%20DAF%20fact%20sheet_final.pdf [Accessed: 2 October 2024].

2. Gartner, "Hype Cycle for Cyber-Risk Management, 2024," 22 July 2024. [Online]. Available: https://www.gartner.com/en/documents/5598859. [Accessed: 2 October 2024].

3. Staff, "CIS Critical Security Controls," n.d. [Online]. Available: https://www.cisecurity.org/controls [Accessed: 3 October 2024].

4. Staff, "Gartner Survey Finds 45% of Organizations Experienced Third Party-Related Business Interruptions During the Past Two Years" 13 December 2023. [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2023-12-13-gartner-survey-finds-45-percent-of-organizations-experienced-third-party-related-business-interruptions-during-the-past-two-years [Accessed: 2 October 2024].

5. Gurpreet Singh Jodhka, "Best of Breed vs Platform Based: The age-old Cybersecurity Dilemma," 26 February 2024. [Online]. Available: https://www.linkedin.com/pulse/best-breed-vs-platform-based-age-old-cybersecurity-dilemma-jodhka-n7xuc/ [Accessed: 26 September 2024].

6. Bank of England, "PS6/21 | CP29/19 | DP1/18 Operational Resilience: Impact tolerances for important business services" [Online]. Available: https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper [Accessed: 26 September 2024].

7. Australian Prudential Regulation Authority, "Enforcement," n.d. [Online]. Available: https://www.apra.gov.au/enforcement [Accessed: 26 September 2024].

8. European Insurance and Occupational Pensions Authority, "Digital Operational Resilience Act (DORA)," n.d. [Online]. Available: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en [Accessed: 26 September 2024].

9. Financial Conduct Authority, "PS21/3 Building operational resilience," 29 March 2021. [Online]. Available: https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience [Accessed: 26 September 2024].

10. Hong Kong Monetary Authority, "Supervisory Policy Manual (SPM): New module OR-2 on "Operational Resilience" and revised module TM-G-2 on "Business Continuity Planning," 31 May 2022. [Online]. Available: https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220531e1.pdf [Accessed: 26 September 2024].

11. Monetary Authority of Singapore, "Guidelines on Business Continuity Management," 06 June 2022. [Online]. Available: https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management [Accessed: 26 September 2024].

Contact us

Rob Boshonek
Deloitte US
Advisory Managing Director
Deloitte & Touche LLP
rboshonek@deloitte.com

Will Burns
Deloitte US
Advisory Managing Director
Deloitte & Touche LLP
wburns@deloitte.com

Kero Bernaba
Deloitte US
Senior Manager
Deloitte & Touche LLP
kbernaba@deloitte.com

Clare Mohr
Deloitte US
Senior Manager
Deloitte & Touche LLP
clmohr@deloitte.com

Emily Notariano
Deloitte US
Senior Consultant
Deloitte & Touche LLP
enotariano@deloitte.com

Taryn Campion
Deloitte US
Consultant
Deloitte & Touche LLP
tacampion@deloitte.com

Deloitte.