



MARTA CHODYKA

John Paul II University in Biala Podlaska,
Poland

ORCID iD: 0000-0002-8819-2451

TOMASZ GRUDNIEWSKI

John Paul II University in Biala Podlaska,
Poland

ORCID iD: 0000-0003-3394-8992

ZBIGNIEW CIEKANOWSKI

John Paul II University in Biala Podlaska,
Poland

ORCID iD: 0000-0002-0549-894X

DIGITAL RESILIENCE OF AN ORGANIZATION IN RISK MANAGEMENT

ABSTRACT

This article explores how organisations can strengthen their digital resilience by managing risks associated with their IT networks. The analysis focuses on practical network design measures – such as using backup links to maintain connectivity, dividing networks into separate zones with specific access controls, and implementing centralised security monitoring tools – to improve both day-to-day operations and responses to incidents. The study uses a simulated business network to test scenarios like link failures, attempts to bypass security zones, and suspicious user activity. Results show that having redundant connections minimises downtime when failures occur, network segmentation blocks unauthorised access between different parts of the network, and central monitoring tools quickly detect and classify unusual activity. By setting up backup systems and dividing the network into separate zones, organisations can avoid big disruptions, cut down on the effects of cyberattacks, and deal with issues faster. These measures help keep operations steady, even when unexpected digital problems come up.

KEYWORDS: organisational digital resilience, cybersecurity risk management, network segmentation (VLAN), incident monitoring (SIEM), Zero Trust principle

INTRODUCTION

Today's businesses rely heavily on dependable IT systems to keep operations running smoothly. When these systems are disrupted – by events like ransomware – the consequences can be severe, including expensive outages and loss of important data. Recent reports show that nearly half of organisations hit by major incidents experience network downtime, and more than 40% lose data (Akamai Technologies, 2023). Because of this, managing cybersecurity risks is now a central part of keeping organisations secure and resilient. Achieving this resilience means making sure that organisations can keep working even if something fails or a cyberattack happens. Key steps include removing single points of failure, dividing networks into separate segments, and improving how incidents are detected (NIST, 2011; Annarelli et al., 2020). The ideas behind these measures aren't new: back in the 1960s, researchers designing early computer networks realised that spreading out critical parts of the system made it much harder for one problem to bring everything down (Baran, 1964). The Internet was originally designed with reliability in mind, rather than

security (Bellovin, 1989). Early versions of the Internet didn't include many safety features, which made them open to attacks (Bellovin, 1989). Over time, as more risks appeared, new protections such as firewalls and encryption were added to strengthen online security (Bellovin, 1989; Scarfone & Hoffman, 2009).

Security strategies today recognise that dangers can come from both outside and inside an organisation's network. Simply putting a strong firewall at the network's edge isn't enough, since many threats – including those from people who already have access – can bypass these defences. The old approach of trusting all traffic within the network no longer works, because attackers who get in can move around freely if there aren't additional controls in place (Kim & Solomon, 2018). The Zero Trust model has become popular as a result. It means that no part of the network is automatically trusted, whether it's inside or outside. Instead, every access request must be checked and approved, and the network is divided into separate segments with strict controls and constant monitoring to keep things secure (Rose et al., 2020; Ahn et al., 2024; Chodyka, 2025).

For organisations looking to reduce risks, having a resilient IT setup is critical. This means putting several layers of protection in place, not just relying on one tool or strategy. These layers include making sure systems stay available even if something breaks, limiting who can access what parts of the network, and having good monitoring in place to catch problems quickly (NIST, 2011; Rose et al., 2020; Chandramouli et al., 2022). This article aims to show, from both a technical and management perspective, how investments in backup systems, network segmentation, and monitoring tools can make an organisation more resilient. First, it outlines how the research was carried out, then it shares the main findings about network reliability, access controls, and threat detection, and finally it discusses what these results mean for security planning.

RESEARCH METHODOLOGY

Organisations today need to be able to keep running even when unexpected problems strike. Researchers have shown that digital tools and information systems can help businesses stay flexible and stable in the face of disruptions (Heeks & Ospina, 2018). Building on their ideas, this study set up a practical experiment to see how certain technical solutions can improve an organisation's

resilience. First, we reviewed existing research on IT security and risk management to understand the foundations. Then, we built a simulated company network similar to what small or medium-sized businesses use. We built the test network with backup internet links, split it into different sections using VLANs, and set up a central monitoring system to spot anything out of the ordinary. The goal was to see how these straightforward tools could reduce risks and help a business keep operating, even if something went wrong or a cyberattack occurred.

We set up a virtual company network in GNS3 to try out these ideas. The layout had a DMZ with a jump host for secure admin access, a user zone, a server area for monitoring, and a separate management section. Routers used AlmaLinux and firewalls, and computers ran on either AlmaLinux or Windows. We made sure every main computer sent its logs to the SIEM using the Wazuh agent, and network devices forwarded their logs too. This made it possible to watch how everything worked under different test situations.

Once everything was set up, we put the network through its paces with a few realistic challenges. We started by disconnecting the main connection to see if the backup would take over smoothly. Then, we checked if the VLANs and firewalls really stopped traffic from crossing into zones where it shouldn't go. For the last test, we tried breaking the rules – trying to get access we weren't supposed to have – to find out if the monitoring system would catch any suspicious activity. During all of this, we watched for how quickly the network recovered, if any data went missing, what the firewalls blocked, and what alerts popped up in the SIEM system. Finally, we compared what happened in our tests with both our expectations and industry-standard threat frameworks like MITRE ATT&CK (MITRE, 2023; Ahn et al., 2024).

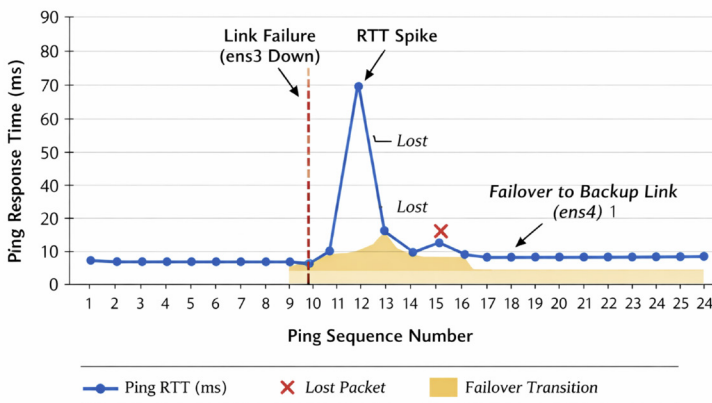
It's important to note that all the tests used fake data and safe, simulated attacks. Everything happened in a controlled lab setting, not on real business systems or with any personal information. This approach allowed us to assess how well the security measures worked without risking real-world issues or exposing sensitive data.

RESULTS

INFRASTRUCTURE RESILIENCE

We started by testing what happens when the main network connection goes down. The system was set up so that if the primary line failed, a backup would automatically take over. In our test, when we simulated a failure, only 2 out of 24 test messages were lost-meaning there was just a short, noticeable blip (about two seconds) before things returned to normal. The short spike in response time quickly smoothed out once the backup kicked in. The chart in Figure 1 shows this brief interruption and the rapid recovery.

Figure 1. *ICMP connectivity continuity during a link failure (redundancy test)*



Source: author's own elaboration based on test data.

No one had to step in and fix the problem – the system handled the switch on its own. After the failover, everything worked as usual, with stable and fast connections, showing that having a backup line really does keep things running smoothly if the main one fails. In our setup, we made sure that every backup network link was plugged into a separate switch, and we set up a dedicated management network just for admin access (Bajpai, 2019). This way, if a switch or section of the network failed, there was always another route available for staying connected and handling problems. Simple choices like

these – using more than one switch and having separate channels for management – make a big difference in keeping everything online (Bajpai, 2019). When we ran the test, our design proved reliable: the network stayed up with barely any interruption, so users could keep working without noticing a thing.

NETWORK SEGMENTATION AND ACCESS CONTROL

The next set of results pertained to network segmentation and restrictive access controls. The enterprise network was divided into multiple security zones (segments) with distinct trust levels: a demilitarised zone (DMZ) for external-facing services, an internal user LAN, an internal server segment, and a separate management segment. Each zone was implemented as a separate VLAN and IP subnet with its own access control policies on the routers. Table 1 summarises the VLAN ID and IP range for each key segment in the test environment.

Table 1. *Example IP addressing and security-zone assignment for key network segments*

Segment (Security zone)	VLAN ID	IP addressing
DMZ (demilitarized zone)	2	10.0.2.0/24
User network (LAN)	3	10.0.3.0/24
Internal server network	5	10.0.5.0/24
Management network	4	10.0.4.0/24

Source: author's own elaboration.

We tested our network segmentation by running two practical scenarios. First, we checked if a regular user computer (User1, VLAN 3) could reach the management network by sending a simple ping. As planned, the firewall stopped all attempts – none of the five test pings got through, and the system replied with *Packet filtered*. This showed that users were blocked from accessing the management area, just as the security policy intended. Using filtered responses instead of clear errors also helps hide extra information about the network from anyone trying to probe it (Scarfone & Hoffman, 2009).

Second, we looked at how admin access worked by using a jump host (also called a bastion host). We tried to connect to an internal server (Server1) both directly from the user network and through the special jump host in

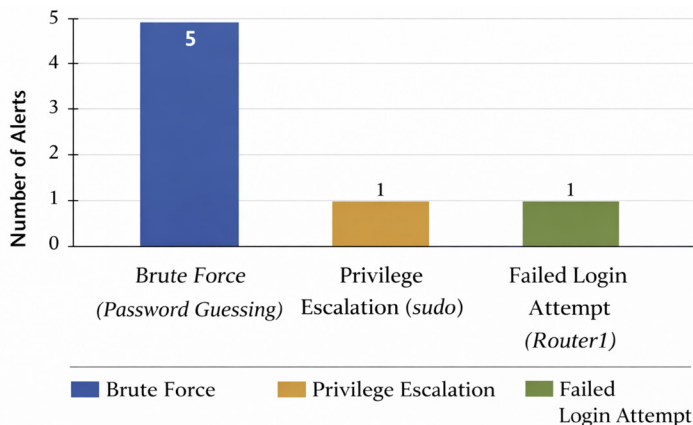
the DMZ (Jumphost1, VLAN 2). Direct access was blocked, but connecting through the jump host was allowed. This means that services like SSH were only available to a specific, trusted source, not to everyone on the user network (Rose et al., 2020; Chandramouli et al., 2022). These hands-on results show that using VLAN separation and focused firewall rules really can limit network access and enforce least-privilege connections between different parts of the network (ENISA, 2022; Rose et al., 2020; Sunkara, 2024).

THREAT MONITORING AND SIEM ALERTS

The last part of our results focused on how well our security monitoring worked. We used the Wazuh system to collect and analyse logs from all over the network. This setup let us see what was happening across every computer and device, using both agents and direct log forwarding from network equipment. With everything in one place, we could easily spot unusual activity or security issues (Kent & Souppaya, 2006; Chandramouli et al., 2022). We ran three practical scenarios to see if our monitoring setup would catch signs of real-world security problems. First, we tried to guess passwords on the jump host to mimic someone trying to break in. Second, we ran a command with admin rights on a normal user computer to test for privilege escalation. Third, we forced a failed login on a router and sent that info to the monitoring system. These tests helped us check if the monitoring really picked up on these risky actions. The results were clear: in the first test, Wazuh quickly alerted us to the repeated failed password attempts and flagged them as suspicious, matching a known attack pattern (MITRE, 2023; Ahn et al., 2024). In the second test, the system noticed when someone tried to use admin rights without permission (Ahn et al., 2024; Kent & Souppaya, 2006). And in the third test, the failed login from the router was caught and logged by the monitoring system, proving it could handle device logs as well as computer logs (Kent & Souppaya, 2006). During these tests, the password-guessing scenario generated several alerts, while the privilege-escalation and router-login failures each triggered a single alert. This pattern makes sense, as repeated suspicious actions are more likely to generate multiple warnings (Kent & Souppaya, 2006). Having all this information in one place made it much easier to spot and

respond to potential problems quickly. Figure 2 shows the number of alerts generated by each scenario.

Figure 2. Recorded security events in the analyzed infrastructure (number of SIEM alerts)



Source: author's own elaboration based on SIEM logs.

These results show that our Wazuh monitoring system can quickly spot both repeated suspicious actions, such as many failed logins, and single unusual events, such as someone suddenly gaining extra privileges or a device login error. By matching these events to known attack patterns, the alerts were easier to understand and act on (MITRE, 2023; Ahn et al., 2024). Overall, the monitoring made it much faster and simpler to detect and analyse security issues, even when the tests were simple simulations.

DISCUSSION

REDUNDANCY AND SERVICE CONTINUITY

Our failover tests clearly showed that having backup network connections makes a big difference in keeping services available. By removing single points of failure, we prevented outages and kept interruptions extremely brief. For example, when the main connection failed in our experiment, the backup link took over almost instantly. Only two pings were lost, so users didn't

notice any real downtime. This kind of setup follows industry best practices – using redundancy to ensure important systems stay up and running even if something breaks (NIST, 2011; Chandramouli et al., 2022).

It's important to remember that even a short network problem can be expensive and disruptive. Some studies put the cost of downtime at nearly \$9,000 per minute (Ponemon Institute, 2016). That's why having backup systems isn't just a technical choice – it's a smart business move. With automatic failover, we kept services running for users and avoided the domino effect of lost revenue or unhappy customers. Our example shows that investing in backup links and other redundant hardware is well worth it for keeping a business running smoothly (Ponemon Institute, 2016).

We also added extra layers of backup in our test, like connecting each network cable to a different switch and using a separate management network for admin access (Bajpai, 2019). This setup means that if one switch or part of the network fails, there's always another way to stay connected and manage the systems. These decisions go beyond just following technical rules – they're smart strategies to keep everything running, no matter what goes wrong. Our results show that treating redundancy as a key part of risk management lets organisations keep working even if something breaks. In short, building in extra connections and management paths makes a big difference in staying resilient against problems and keeping downtime to a minimum (NIST, 2011; Bajpai, 2019).

SEGMENTATION AND ATTACK SURFACE REDUCTION

Our tests showed how breaking a network into separate zones and tightly controlling traffic between them makes the whole system more secure. For example, when we tried to access the management network from the regular LAN, it didn't work – users couldn't get through, and admin servers were only accessible via a special jump host. This setup means that even if someone breaks into one part of the network, they can't easily move around or reach the most sensitive systems (Rose et al., 2020; ENISA, 2022). It's like having firebreaks in a forest – any trouble is contained and can't spread everywhere.

From a risk perspective, using VLANs and firewalls reduces the likelihood that an attacker can reach critical systems or cause widespread damage

(Sunkara, 2024; ENISA, 2022). If someone manages to get into one part of the network, they still run into several more barriers, like not being able to ping or access management or server networks. Each extra layer makes it harder and slower for an attacker, giving defenders a better chance to notice and stop them (Rose et al., 2020). In our case, malware on one compromised computer couldn't infect other network areas because traffic between segments was blocked. This approach prevents security problems from spreading and aligns with what's seen in real businesses – networks that use fine-grained segmentation are better at containing incidents and limiting losses than flat networks (ENISA, 2022; Sunkara, 2024). Our results back this up: segmenting key network areas helped reduce both how long and how far a breach could go.

The way we set up segmentation also follows the Zero Trust security model, which means no one is automatically trusted and everyone needs to prove they should have access (Rose et al., 2020; Ahn et al., 2024; Chodyka, 2025). For example, admin access to servers only worked through a special jump host with strict controls – users couldn't just connect directly (Rose et al., 2020; Chandramouli et al., 2022). This approach means even insiders or hacked accounts can't move freely across the network. Our tests confirmed this: unauthorised attempts to access sensitive systems were blocked every time. Keeping tight controls between network segments makes it much harder for attackers to get to important resources – even if they're already inside the network (Rose et al., 2020; ENISA, 2022).

By keeping important systems separate and limiting what users can do, the organisation also meets industry standards and regulations. Guidelines from groups like ENISA and NIST recommend network segmentation to protect sensitive data and ensure people only access what they truly need (ENISA, 2022; Chandramouli et al., 2022). In areas like finance and healthcare, these rules are often required by law. Our setup worked as intended: the management part of the network was completely cut off from regular user PCs. That not only protects key systems, but also makes it much harder for an attacker who gets into one machine to move on to anything more important. Any attempts to scan or connect to restricted areas were blocked outright and could be tracked as suspicious activity. In short, segmentation puts up multiple walls so even if someone gets in, they can't easily reach the most valuable systems.

To sum up, segmenting a network makes it much harder for attackers to move freely or reach sensitive systems, and it limits how much damage they can do if they get in (Rose et al., 2020; ENISA, 2022; Sunkara, 2024). It's like having firebreaks inside the network – problems are contained, and defenders get more time to spot and stop them. Our hands-on tests show that this strategy really works and should be a top priority for any organisation that wants to be more resilient against cyber threats. Designing your network with separate zones, strict access rules, and dedicated admin paths isn't just smart – it's one of the best ways to reduce risk and prevent attacks from spreading out of control (Rose et al., 2020; ENISA, 2022; Chandramouli et al., 2022).

SIEM MONITORING AND DETECTION CAPABILITIES

Adding the Wazuh SIEM to our setup made it much easier and quicker to spot and react to security problems. In our tests, the SIEM picked up on incidents almost instantly, which is a huge step up from the industry average, where it can take months to even notice a breach (IBM Security, 2023). Quick alerts mean you can fix issues before they cause real harm. For example, when our system spotted just a few failed login attempts, it immediately raised a red flag. This kind of speed is key to keeping problems small and manageable, instead of letting them grow unnoticed (IBM Security, 2023).

The SIEM didn't just send out alerts – it gave us useful details about what was happening. For example, it could tell the difference between someone trying to brute-force a password and someone suddenly getting admin rights (MITRE, 2023; Ahn et al., 2024). It matched these alerts to known attack types, making it easier for us to understand and act fast (MITRE, 2023; Ahn et al., 2024). You don't need a giant security team for this either; our experience showed that even smaller organisations can get these benefits by using the right tools. The SIEM kept an eye on everything and let us know right away if anything looked suspicious.

Having all our security data gathered in one spot changed how we worked. Before we brought in a SIEM, tracking down issues meant digging through logs scattered across various computers and devices – it was time-consuming and sometimes frustrating (Kent & Souppaya, 2006). Once we started using Wazuh, we could see everything at a glance on a single dashboard (Kent & Souppaya, 2006).

Issues like failed admin commands or devices dropping offline stood out right away, so we could react quickly and keep anything suspicious from slipping by unnoticed.

From a risk management perspective, SIEM monitoring lets you spot trouble quickly and act before it becomes a crisis (Kent & Souppaya, 2006; IBM Security, 2023). Instead of reacting after the fact, you get a chance to stop attacks while they're still unfolding. For example, if ransomware starts on one computer, a quick alert lets you step in before it spreads. Our tests showed that fast alerts give you time to lock accounts or disconnect affected machines, stopping bigger problems before they start. Even with good prevention, some threats will sneak through – it's the monitoring that helps catch and handle them before they get out of control (NIST, 2011; Kent & Souppaya, 2006).

It's important to remember that SIEMs work best when properly set up and managed (Kent & Souppaya, 2006). In our tests, the basic Wazuh setup was sufficient, but in the real world you'd want to fine-tune the rules and define clear steps for handling alerts (Kent & Souppaya, 2006; Chandramouli et al., 2022). An alert by itself doesn't fix a problem – someone has to check it out and decide what action to take, like shutting down an account or disconnecting a device (Kent & Souppaya, 2006). Some systems can even automate these responses. The bottom line is that technology and people have to work together: the SIEM is the alarm, but you still need a good team and a solid plan to respond quickly and effectively (Bagheri et al., 2023; Kent & Souppaya, 2006).

CONCLUSIONS AND IMPLICATIONS

Bringing everything together, our main tools – backup network links, network segmentation, and centralised monitoring – work together to make an organisation more resilient to cyber risks (NIST, 2011; Rose et al., 2020; Chandramouli et al., 2022; Kent & Souppaya, 2006). Backup links keep things running if something fails, segmentation stops attackers from moving easily through the network, and monitoring helps us spot and react to threats quickly. Using these layers together provides much better protection than any one of them alone (NIST, 2011; Annarelli et al., 2020).

We found that these approaches work best when used together. Backups help prevent major outages, splitting the network into zones keeps problems contained, and monitoring makes it easier to catch and fix issues quickly. When you combine these elements, it's much easier for a business to recover from setbacks and maintain steady operations – that's the core of resilience (Annarelli et al., 2020; Bagheri et al., 2023).

But these tools won't do much good on their own unless they're properly looked after. It's crucial to test backups, regularly review how access and network zones are set up, and fine-tune monitoring so you're not overwhelmed by alerts (Chandramouli et al., 2022; Kent & Souppaya, 2006). Just as vital is having a team that knows what to do when something goes wrong. Without good management and a solid response plan, even the best systems can fall short (NIST, 2011; Bagheri et al., 2023).

From a management perspective, this case study shows that smart infrastructure choices can directly reduce risks. Cutting out single points of failure, limiting how far problems can spread, and making it easier to track important activity all help justify these investments – not just as technical upgrades, but as essential parts of business continuity and security policies (Ciekanowski & Wyrębek, 2016; Rose et al., 2020; IBM Security, 2023). In short, building a strong digital foundation helps organisations stay stable and flexible in a changing threat landscape (Heeks & Ospina, 2018; Lu et al., 2025; Singh et al., 2025).

REFERENCES

- Akamai Technologies. (2023, November 6). *Ransomware Attacks Have Doubled Over the Past Two Years, According to Akamai Research* (Press Release). Cambridge, MA: Akamai. Retrieved from Akamai Newsroom.
- Ahn, G., Jang, J., Choi, S., & Shin, D. (2024). Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model with the MITRE ATT&CK Matrix. *IEEE Access*, 12, 89291–89309. <https://doi.org/10.1109/ACCESS.2024.3417182>
- Annarelli, A., Nonino, F., & Palombi, G. (2020). Understanding the management of cyber resilient systems. *Computers & Industrial Engineering*, 149, 106829. <https://doi.org/10.1016/j.cie.2020.106829>
- Bagheri, S., Ridley, G., & Williams, B. (2023). Organisational cyber resilience: Management perspectives. *Australasian Journal of Information Systems*, 27. <https://doi.org/10.3127/ajis.v27i0.4183>
- Bajpai, M. (2019). Optimising network availability through out-of-band configuration change (OOBC) process – Network management for communication service providers. *European Journal of Advances in Engineering and Technology*, 6(11), 90–93.
- Baran, P. (1964). *On Distributed Communications: V. History, Alternative Approaches, and Comparisons* (RM-3097). Santa Monica, CA: RAND Corporation.
- Bellovin, S. M. (1989). Security Problems in the TCP/IP Protocol Suite. *ACM SIGCOMM Computer Communication Review*, 19(2), 32–48. <https://doi.org/10.1145/378444.378449>
- Chandramouli, R., et al. (2022). *Guide to a Secure Enterprise Network Landscape* (NIST SP800-215). Gaithersburg, MD: National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-215>
- Chodyka, M. (2025). Security analysis of public administration databases in Poland within a Zero-Trust environment. In R. Szczebiot (Ed.), *Innovation Trends 2025* (pp. 91–99). University of Łomża. ISBN 978-83-60571-75-0
- Ciekanowski, Z., & Wyrębek, H. (2016). Zarządzanie ryzykiem. *De Securitate Et Defensione. O Bezpieczeństwie I Obronności*, 2(2).
- European Union Agency for Cybersecurity (ENISA). (2022). *ENISA Threat Landscape 2022*. <https://doi.org/10.2824/764318>
- Heeks, R., & Ospina, A. V. (2018). Conceptualising the link between information systems and resilience: A developing country field study. *Information Systems Journal*, 29(1), 70–96. <https://doi.org/10.1111/isj.12177>
- IBM Security. (2023). *Cost of a Data Breach Report 2023*. IBM Corporation.
- Kent, K., & Souppaya, M. (2006). *Guide to Computer Security Log Management* (NIST SP800-92). Gaithersburg, MD: NIST. <https://doi.org/10.6028/NIST.SP.800-92>
- Kim, D., & Solomon, M. G. (2018). *Fundamentals of Information Systems Security* (3rd ed.). Jones & Bartlett Learning.

- Lu, J., Wang, X., Feng, Y., & Liu, L. (2025). Surviving and thriving: An organisational resilience framework in the digital age. *Industrial Management & Data Systems*. Advance online publication. <https://doi.org/10.1108/IMDS-10-2024-1044>
- MITRE. (2023). *MITRE ATT&CK® Technique T1110.001 – Password Guessing*. Retrieved from <https://attack.mitre.org/techniques/T1110/001/>
- National Institute of Standards and Technology (NIST). (2011). *Managing Information Security Risk: Organisation, Mission, and Information System View* (NIST SP800-39). Gaithersburg, MD: NIST.
- Ponemon Institute. (2016). *Cost of Data Centre Outages* (Research report; sponsored by Vertiv). Ponemon Institute LLC.
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero Trust Architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-207>
- Scarfone, K., & Hoffman, P. (2009). *Guidelines on Firewalls and Firewall Policy* (NIST SP800-41Rev.1). Gaithersburg, MD: NIST.
- Singh, K., Chatterjee, S., Mariani, M., & Fosso Wamba, S. (2025). Cybersecurity resilience and innovation ecosystems for sustainable business excellence: Examining the dramatic changes in the macroeconomic business environment. *Technovation*, 143, 103219. <https://doi.org/10.1016/j.technovation.2025.103219>
- Sunkara, G. (2024). The Importance of Network Segmentation in Security. *International Journal of Engineering and Technical Research*, 8(3), 45–53. <https://doi.org/10.5281/zenodo.15792900>
- Verizon. (2023). *2023 Data Breach Investigations Report (DBIR)*. New York, NY: Verizon Enterprise. Retrieved from <https://www.verizon.com/business/resources/reports/dbir/2023>