

Research and case scenario in Data Security and Compliance

Hasan Sivas

2421062

Task 1 – Research in Data Security and Compliance	2
Introduction	2
Main	2
Conclusion	6
Task 2 – Case Scenario	7
Introduction	7
Main	8
Conclusion	13
bibliography	14

Task 1 – Research in Data Security and Compliance

Introduction

In recent years, especially since the beginning of the COVID-19 pandemic in late 2019, more and more companies have begun to realise the benefits of providing employees with hybrid work and work-from-home schemes. According to the Stanford Research Institute, about 42% of the workforce in America works from home at least one day a week [7]. The potential benefits of working from home include: increased employee satisfaction (which would typically lead to better employee performance and reduced turnover), less time wasted on commuting and improved organisational flexibility [2]. However, remote and hybrid work is not without its downsides; As the network is extended to less secure locations, the surface for attack grows, providing more opportunities for hackers and other threats to land a successful attack.

With the increase in remote work, attack surfaces have been growing whilst at the same time, companies have been growing more aware and integrating more cyber hygiene practices into their policies, including security awareness training, acceptable use policies, and basic technical controls. These measures are often implemented inconsistently and rely heavily on employee compliance, and as a result, are often failed to be implemented unilaterally [7]. In other words, there is often a gap between an organisation's

understanding of best security practices and its actual implementation of them.

This paper will seek to uncover the potential security pitfalls associated with remote work as well as the myriad of solutions organisations have come up with to deal with them and built upon over time in a back-and-forth arms race with threat actors. By analysing best practices in both technological controls and security procedures implemented by well-established corporations and guidelines (Cloudflare, ISO27000, IBM etc..), this paper will seek to highlight how to create modern systems that respond to threats dynamically and automatically. In particular, it will cover the use of contemporary security models such as Zero Trust Network Access (ZTNA), Secure Access Service Edge (SASE), as well as network implementations such as VPNs, IDPS and Next Generation Firewalls that have become essential cybersecurity fixtures.

Main

To start out with, a large variety of threats arise when a company begins supporting remote work.

The most obvious issue is the potential for connection via unsecured networks. Most employees at a given company may not be IT experts and their home networks may not be as secure as the office's, the hub

may be old, or they may be using default passwords, which can be easily found online. Issues can also arise when employees try to fix IT issues themselves but do so in a way that may not be perfect and leave vulnerabilities, this is referred to as shadow IT [7]. Even if the employee in question has a good understanding of digital hygiene, they may still pose an increased risk due to the actions of others using the same home network. If an employee is connecting via unsecured wifi, data being transmitted may be vulnerable to interception e.g. via Man-in-the-Middle attacks, this is potentially very dangerous as the lack of in-person interaction being standard means that hackers are able to get a greater mileage out of any stolen credentials.

In cases where an employee is accessing the company network through public wifi, there is even greater danger. These networks are typically open, poorly monitored, and used by a large number of unknown people. Public wifi access points such as cafés, airports, or hotels are for this reason, common targets for attackers, who may deploy rogue access points (hotspots set up by hackers disguised as legitimate ones) or exploit weak encryption to intercept packets from these users[9]. Using signature-based IDPSs (intrusion detection and prevention systems) may be advantageous, signature-based tools such as SNORT can detect rogue AP-based attacks with a 91% detection rate[9].

Bring your own device to work (BYOD) policies also pose a potential risk[7]. In hybrid work systems, employees may sometimes be encouraged or permitted to bring their own devices from home to work, allowing for productivity to occur

seamlessly. The issue is that as these devices are not company property and are not monitored by the same systems as other devices on the networks or the company's IT professionals. Their applications may not be updated to the appropriate version, they may not be using antivirus and therefore there is a risk of the employee unintentionally compromising the network by introducing malware. A simple solution to this is to offer devices which employees can take home, however this may be too costly for smaller companies.

Due to the aforementioned lack of IT oversight, man-in-the-middle attacks are a more common risk when it comes to working from home, as attackers can position themselves between employees and corporate resources without being detected. This means that hackers may be able to intercept sensitive communications, manipulate transmitted data, or harvest the employee's credentials, which can then be reused to gain unauthorised access and move laterally throughout the network.

Cyber Hygiene Factor	Positive Practice Group	Negative Practice Group	Difference
Software Updates	Update Monthly/Weekly (61.8%)	Rarely/Never (38.2%)	23.6% gap
Two-Factor Authentication (2FA)	Always (50.9%)	Sometimes/Never (49.1%)	25% gap
Data Backup	Regular (63%)	Irregular/No Backup (37%)	26% gap
Security Tools Usage	Use Antivirus/Firewall/VPN (70.9%)	None (29.1%)	29% gap
Password Management	Strong Passwords Remembered (49.1%)	Weak/Repeated Passwords (50.9%)	30% gap

Fig A. Table from [7] showing the disparity between people actually implementing security practices after training.

A simple solution to many of these threats is to educate employees on cyber hygiene and provide training for those who work from home. Overall, it seems that the employee's personal values and personality affect security just as much as formal policies [5]. It is clear that while it is important that a significant amount of attention is given to keeping employees informed and well-trained, there will still be issues that this will not cover. It is key that in addition to training, many physical and or software measures are placed to bolster any network's defences.

However, despite the great number of threats, there are many tools and strategies which have enabled companies to continue practising remote work securely.

Virtual Private Networks (VPNS) have become an essential tool in enabling remote work to be feasible at all. VPNS encrypt incoming traffic and secure remote access instances against untrusted networks[10], VPNs form encrypted tunnels between remote devices and corporate gateways, allowing the network to be extended anywhere. This encryption helps mitigate against potential man-in-the-middle attacks by preventing attackers from intercepting or modifying ongoing traffic, even if they are positioned on the same network. As a result, VPNs allow companies to provide remote access to devices on the network whilst maintaining the same level of confidentiality and integrity of transmitted data as before.

VPNs alone, however, are not enough to secure hybrid work traffic. The

encrypted nature of VPNs means that end-to-end traffic isn't fully visible to IT, allowing for potential threats to develop unchecked. Because there is implicit trust, they also by themselves do not protect against credential theft or lateral movement of intruders once they've gained access to a session (e.g. via credential theft, hacking or physically accessing the device). Classical models (often referred to as castle and moat[6]) typically rely on just VPNs and Firewalls to protect the network. To fully secure the remote network in the ever-evolving threat landscape, a more modern and robust solution is mandatory.

Zero Trust Network Access (ZTNA) and the broader concept of Zero Trust [3] have been adopted with great effectiveness by many organisations to strengthen information security. The core principle of Zero Trust is that nothing is trusted by default; devices, end users, and processes are all treated as potential threat vectors unless explicitly verified.

Key features of Zero Trust include end-to-end secured communications, session-based resource allocation, strict authentication and authorisation of users and devices, and continuous monitoring of network-associated assets. One of the most critical features of ZTNA is that each application surface is verified independently. Unlike traditional network security models, where connecting to the network (for example, via a VPN) can grant broad or full access, ZTNA access decisions are made per request for a single application only. Successfully authenticating to component A does not automatically grant access to component

B; for example, access to a Moodle system does not imply access to email services or internal APIs. Each application enforces its own access policies based on identity and context, significantly limiting lateral movement and ensuring that any mistakenly granted access results in minimal potential damage.

ZTNA are often incorporated into cloud-based solutions, a good example of which is Secure Access Service Edge, or SASE. SASE is a cloud-based architecture solution which centralises controls on the cloud-based network edge (cloud edge)[6] and incorporates ZTNA into its model, and all its associated no-trust features. The network edge is the boundary where the internal network connects to the external network, with SASE the edge being cloud-based means that security is as close as possible to the remote working end user, meaning there is less latency and greater protection.

Next Generation Firewalls (NGFW) are key components in the network that help to continuously scan for issues as they arise. Unlike legacy firewalls which operate primarily at the network and transport layers, NGFWs incorporate deep packet inspection(examining the actual content of the packets), application awareness, intrusion prevention, and threat intelligence to identify and block malicious activity in real time.

Much like a firewall, Intrusion Detection Systems (IDPS) also function by perpetually scanning the network for anomalous activity via the monitoring ingoing and outgoing network traffic.

Unlike a firewall, however, IDPSs detect and analyse behaviour instead of simply restricting traffic based on access rules. IDPSs can be network-based or host-based but for the complexity of networks that account for hybrid work, a hybrid IDPs is more suitable. Although this means IDPSs will generate many false positives, this is acceptable. From a security perspective, a false negative is much less desirable than a false positive, as the consequences of ignoring a potential breach are much more costly; it is therefore preferable for an IDPS to flag many false positives rather than let threats slip through.

Another popular line of defence is the use of honeypots. A honeypot is a decoy system that poses itself as a network-often with intentional vulnerabilities to lure the attention of cybercriminals away from the actual main systems to waste their time and resources, act as a decoy and provide more time for a response during attacks. Honeypots also allow security teams to gather information about the latest attacking strategies, obtained data can be used to strengthen the network's IDPSs and Endpoint Detection Response. Organisations place honeypots in 'demilitarised zones', these are remote-access networks that are made to actual functioning nextworks with simulated traffic but are isolated via firewalls or VLANs so that there is no risk of damage[11].

In some instances, systems of multiple honeypots called 'honeynets' are used. These hosts actually run applications and services to more convincingly mimic the appearance of an actual network and lure more attackers

A potential risk with remote work is the possibility of violating guidelines such as the GDPR, therefore Data Loss Prevention (DLP) plays an essential role in these systems. Personal information may potentially be at risk if remote working employees handle them unsecured areas or through interception/man-in-the-middle attacks.

Data Loss Prevention tools are essential in order to make sure data is handled legally and without compromise to its Confidentiality, Integrity or Availability. The ISO27000[4] provides key guidelines that help with regulatory compliance by providing a risk-based framework for managing information security and implementing security policies and access levels. These include standards for monitoring, measurement and analysis(auditing), risk management techniques and guidelines for auditors. Together, these measures help ensure that remote work practices remain compliant, auditable, and resilient against data breaches.

Future developments in safeguarding hybrid workplaces may involve the incorporation of fast-growing AI technologies. Endpoint Detection and Response is a framework that uses advanced analytics in the form of AI to monitor endpoint threats, respond automatically and then incorporate the incident into its dataset[10]. AI cybersecurity may allow for faster and more adaptive security in the long run, however, it may be dangerous to have a completely zero-touch system with no human oversight.

Conclusion

Remote and hybrid work has become an increasingly common feature of the modern world, starting in the 2020s. Stemming from the lack of IT oversight and managed infrastructure, many issues and vulnerabilities may arise when a company transitions to enable remote or hybrid work. Potential issues may include employees connecting to the company network through unsecured networks, increased susceptibility to phishing scams, the compromising of information's confidentiality, improperly maintained/unpatched software and increased leeway for hackers to move laterally with compromised credentials.

It is evident that training is currently a significant limiting factor in making remote working safe, as many do not show improvements in behavior afterwards. Although technological implementations can help secure the network the actual safety of working from home will not significantly improve without instilling proper cyber hygiene by improving training methods.

Although it creates new issues, the benefits mean that it is and will continue to be worthwhile for companies to invest in remote working and ways to make it more secure. Many models and technologies have been developed for safeguarding networks, many of which can be used to resolve or reduce the risks brought about by remote working.

A key step towards making remote work more sustainable is the development of Zero Trust models. By maintaining a “no trust” policy and making context-aware access decisions whilst continuously monitoring user behaviour, ZTNA reduces the risk of credential misuse, lateral movement of hackers throughout the network, and stops threats going unchecked in hybrid work environments.

Cloud-based architectures such as SASE also bolster security by centralising operations around networks based on the cloud rather than servers located at the company. By centralising policy enforcement, monitoring, and threat detection at the cloud edge, SASE provides consistent protection for users regardless of their location or network and makes remote work more scalable than traditional jobs.

Data Loss Prevention (DLP) plays a critical role in protecting sensitive information and obeying legal guidelines in remote and hybrid work environments, where data is frequently accessed, transmitted, and stored outside the office and is at greater risk. By enforcing security policies that control how data can be shared or transferred, DLP helps mitigate the risk of accidental data leakage caused by human error, compromised credentials, or insecure networks.

As they look to the future and the ever evolving threatscape, many companies are looking into AI-based solutions for further strengthening security, such as Endpoint Detection and Response (EDR), which may make networks stronger and more adaptive than ever towards threats, but could potentially leave flaws that would go unnoticed without human interference.

Task 2 – Case Scenario

Introduction

ResilientIntellect Ltd is a threat intelligence and consultancy company seeking to expand its business into the EU by forming a brand new unit. As a tech company, there are many guidelines, regulations and laws that ResilientIntellect will need to be aware of when establishing its new European unit, such as the Digital Operational Resilience Act (DORA) regulations and the Network and Information Security Directive (NIS2). ResilientIntellect (ResInt)’s main avenue of business is assisting businesses to strengthen their cybersecurity by providing consultation on tools, frameworks, regulatory compliance and by creating AI-powered threat analysis software.

Because of the sensitive nature of its business, it is therefore notable that the company has a very low risk appetite towards the confidentiality of its information being compromised; It would be in the company’s best interest to develop a new, strict information security policy which adheres to the requirements for IT business in the EU and provide the necessary training to make sure that employees follow them. This paper will provide an example of a potential security policy, based on already existing frameworks.

Due to the hybrid nature of ResilientIntellect’s work environment, with presumably many employees working from outside of the EU office on any given day, many safety considerations will need to be taken into account in the planning of its new infrastructure in order to minimise the risks brought about by remote work and create a robust and secure network. For this reason, this paper will suggest and outline the development of more modern solutions, based on models such as Zero Trust Network Access (ZTNA)/(ZTA), which seek to maximise security as much as possible by minimising trust in a given session [3]. continuous verification, least privilege access, and assumption of breach are well-suited to ResilientIntellect’s hybrid workforce.

For improved scalability to meet ResInt’s high potential for growth and to maximise compatibility with ZTA, it would also be beneficial to outline a cloud-based architecture, such as SaaS (Software as a Service)[16]. Cloud-native platforms offer elastic scaling to support ResilientIntellect’s projected growth within the EU, while enabling strong integration with Zero Trust controls such as identity providers, conditional access, and continuous monitoring and SaaS in particular supports the hosting of AI and machine learning apps.

Main

A.Design

For many reasons, it would be beneficial to have a Zero Trust approach to design when it comes to ResInt’s EU Unit. ‘Zero Trust’ is a concept first outlined by John Kindervag in 2009[3], and it can be summed up as the principle that no user, device or process is trusted by default.

As outlined it in task 1, traditional security models are less secure because once they gain authentication, hackers can move laterally across systems, increasing the potential for intruders to find sensitive information, which could result in loss of assets (plans and advice given to clients may need to be scrapped and reimbursed), loss of reputation and loss of business. ResInt’s assets may also be more likely to get attacked due to the hybrid business model, NIS2 explicitly recognises remote access as a significant attack vector[14], requiring organisations to apply consistent security controls regardless of network location. ResInt’s Zero trust systems will restrict movement, assuming all instances the be equal to a breach and enforcing continuous authentication, per-session authorisation, and least-privilege access unilaterally.

Facet	Implementation
Least-privalege	ResInt will enforce least-privilege access by assigning users role-based permissions that grant them only the minimum level of

	access required to perform their jobs, with privileges reviewed and adjusted dynamically as roles or risk levels change.
Per-session authorisation	Access to ResInt's applications and data will be authorised on a per-session and per app basis(1 login - 1 session), ensuring that authentication to one resource does not implicitly grant access to others and that each access instance is evaluated independently.
Continuous authentication	ResInt will implement continuous authentication by monitoring usage signals such as user behaviour, device security posture, location, and session activity, allowing access decisions to be re-evaluated and revoked in real time if risk level increases.
MFA	MFA will be mandatory for all users accessing ResInt systems, requiring at least two independent authentication factors, typically this will mean inputting password and a hardware or app-based token e.g. receiving a text code when trying to log in. This will significantly reduce the risk of unauthorised access through credential compromise.

Fig B. A table showing how ResInt could implement several facets that contribute to a 'zero trust' system

SaaS can be implemented by hosting ResilientIntellect's core business applications such as collaboration tools, case management systems, and its AI-driven threat analysis platforms in EU-based cloud environments. This can easily be integrated into Zero Trust Access as access to the cloud server can be controlled through identity providers and Zero Trust policies. This approach enables rapid scalability, consistent and security controls while supporting remote access, with the benefit of simplified maintenance due to lack of needing traditional server components in the building. The downside is that this would mean ResInt's EU unit will be dependent on cloud providers and that business may slow down if there is an outage and potentially impact its ability to serve clients in a timely manner.

AI can be leveraged in cloud-based platforms to further improve network automation by implementing automated threat identification and response /EDR[15]. By analysing server-wide network traffic, endpoint telemetry, and behavioural data in real time, AI-driven

systems can gather data on anomalies and indicators of compromise that may evade traditional rule-based security tools and feed it into the Continuous Integration and Development Pipeline CI/CD. When integrated into a SaaS and Zero Trust architecture, these AI-enabled controls can automatically initiate response actions such as isolating compromised endpoints or revoking access tokens. After an attack, AI systems can also automate recovery by initiating automated rollbacks or healing stacks, hastening the return to normal business[15].

In order to assist with gathering further information on threat behaviour whilst also providing an additional layer of defence, it may be in ResInt's interest to set up HonetNets for the EU unit. As described in Task 1, honeynets are chains of multiple honeypots that mimic the appearance of an actual active network to lure in attackers[11]. Data recorded of attacks on these honeynets can then be fed into ResInt's AI model training in order to produce modern and up to date AI-powered threat analysis software. These are often employed by antivirus companies to gather threat intelligence on malware and could be equally useful to ResInt.

B.work Structure

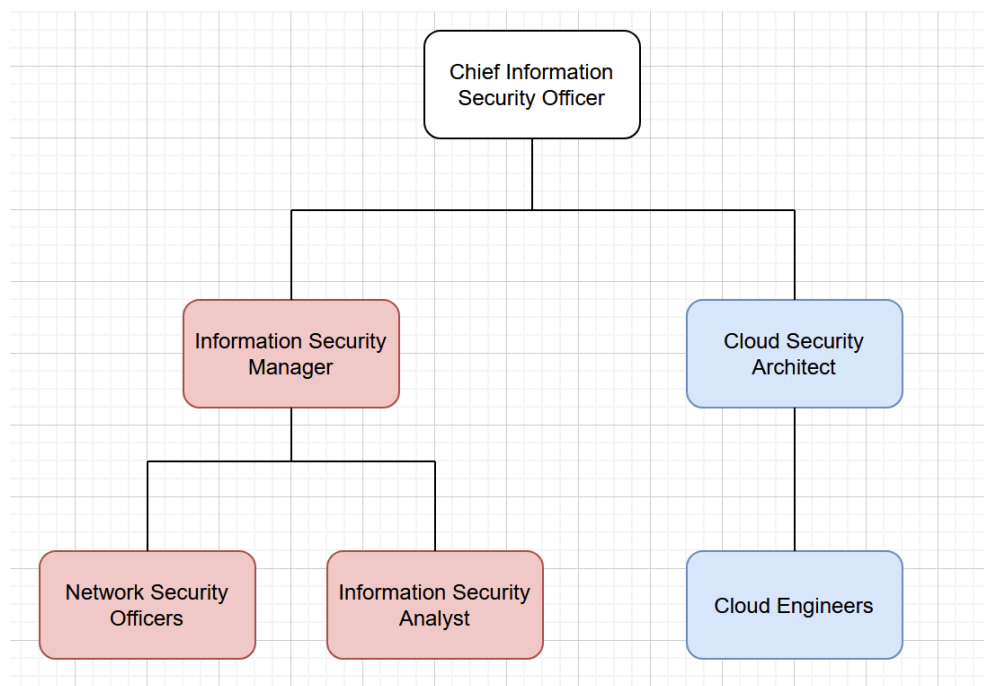


Fig C. A simple chart showing a potential organisational structure for the networking department

In this proposed structure, the Chief Information Security Officer (CISO) holds the most responsibility for the organisation's information security strategies, governance, and risk management. This role will be accountable for aligning security objectives with ResInt's business goals and making sure all operations are compliant with regulatory frameworks and local laws and the maintenance/updating of the security policy.

The Information Security Managers preside over the Network Security officers and Information Security Analysts and are responsible for translating strategic security objectives into operational controls. They oversee Network Security Officers and Information Security Analysts, ensuring that security policies are consistently implemented, monitored, and enforced.

The Cloud Security Architect and cloud engineers are responsible for managing the company's cloud-based network (SaaS). This job involves implementing identity and access management controls, ensuring secure configuration of SaaS platforms, and integrating cloud services with ResInt's Zero Trust and SASE architectures.

During the initial formation of the European unit, it may be necessary to enlist temporary hires or transplant from ResInt's already existing staff, in order to assist with training and the development of the architecture. The actual organisation may therefore not initially resemble Figure C.

C.Policy & Compliance

Policy makes up a massive part of what is needed to ensure ResInt's workforce is conducting business efficiently and securely. A policy is a rule created by a company for its employees to follow. Unlike a law there will not usually be legal consequences for failing to follow a policy, but rather each company may have its own way of reprimanding the employee or dealing with the situation. Not everyone in the office will be familiar with IT or cybersecurity so a good policy is essential to make sure their actions remain within safe parameters.

Security frameworks are well established standard procedures for maintaining good information security practices, e.g., ISO 27000, NIST, CERT/CC and DORA. These are tried and tested practices that are already accepted to work in a wide range of environments and can be personalised to suit a company's specific needs. Some of the rules and guidelines may be generic or not completely suitable for your company, requiring further tailoring.

DORA (Digital Operational Resilience Act) and the NIST (National Institute of Standards and Technology) in particular put forth many guidelines that are relevant to ResInt. Operational Resilience is important, as it ensures that an organisation can continue to deliver critical services during and after disruptive events such as cyberattacks, system failures, or data breaches. In the context of ResInt, where operations rely heavily on cloud-based services and remote access, maintaining resilience requires robust incident response planning, redundancy, and continuous monitoring of systems. The NIST also outlines that organisations must report breaches and other significant incidents in a timely manner, according to the local laws. The UK GDPR specifies that reports breaches likely to cause risk to the rights of individuals must be disclosed no later than 72 hours after they are

discovered[12], following these requirements strictly is essential for ResInt to avoid legal issues and to maintain the trust and cooperation of its EU clients.

Many of the policies in the provided example policy (Seen in Additional Files) are designed to assist in ensuring compliance with DORA. E.g. 5.a. & 5.b. Emphasises the importance of logging and analysing and reporting major incidents to fulfil due diligence and maintain compliance with DORA's article 19[17] and NIST's reporting requirements[14].

In order to ensure its security policies are actually effective, ResilientIntellect must make sure that proper training and education is available for employees on the importance of cyberhygiene and compliance with company policies by implementing a SETA program (Security Education, Training and Awareness)[8]. Security awareness is an important aspect of SETA, it helps ensure that security remains at the forefront of employee's minds and is passively implemented in their daily actions, decreasing the overall chance of lapses in judgement leading to security incidents e.g. falling for phishing scams, using repeated passwords.

D.Risk Management

There are a number of risks that may be present with the proposed design for ResInt's EU unit.

As ResInt develops AI-powered threat analysis software, automatically updating it through CI/CD, the product is at risk of being damaged if there is an issue with the input training data. Data poisoning may occur due to a multitude of reasons such as industrial sabotage or erroneous data collection but is harmful regardless. To mitigate the risk of data poisoning attacks, ResInt should implement multiple defensive controls throughout its SaaS CI/CD pipeline by applying the same Zero Trust principles in the rest of the network to the AI pipelines. All training data traffic should be monitored so that anomalous samples can be flagged for analysis and removed so that they cannot poison the output[15].

As mentioned earlier, due to ResInt's infrastructure being cloud-based, there is a possibility of downtime caused by the cloud service providers. Service outages, regional disruptions, or misconfigurations at the provider level can result in temporary downtime, directly impacting ResInt's ability to deliver services to clients in a timely manner. One potential solution for this may be to use multi region/multi cloud solutions wherein different departments use different cloud providers that interconnect, this means that the entire business is unlikely to be halted all at once but it may however be costly.

E.Contingency planning:

An incident response plan is deployed during or immediately after the incident occurs; the aim is generally to minimise the impact of the incident (minimising operational and reputational impact) and facilitate recovery. Unlike a policy, it is more reactive than proactive [13].

Disaster recovery is deployed after the incident is over. This is the process of verifying the status of assets, conducting repairs, restoring systems ect. As well as documenting the incident for the sake of future policy. Key steps include verifying the integrity and availability of critical business assets, repairing or rebuilding compromised infrastructure, restoring backups, validating system functionality and informing customers of any potential delays.

A business continuity plan entails the key steps that a business needs to undertake to resume normal business in the wake of the occurrence of a disaster. This means ResInt must first identify which employees are needed and capable of beginning the task[13] of assessing the damage done. By documenting what went wrong, why and how it was solved, ResInt can begin to put in safeguards to prevent it from happening again and fulfil DORA requirements.

Together, incident response, disaster recovery, and business continuity will help form a layered approach to ResInt's operational resilience, aligning closely with the objectives of regulatory frameworks such as DORA and allowing it to cope with unforeseen circumstances.

Conclusion

To conclude ResilientIntellect Ltd in its expansion to the EU would benefit greatly from adopting Zero Trust Access architectures and philosophies and a development pipeline centered around cloud computing models, particularly Software as a service (SaaS). These approaches directly address the security challenges posed by ResInt's hybrid workforce, distributed assets, and usage of sensitive threat intelligence and client data by minimizing a trust and enabling a seamless entirely cloud hosted network to host development applications.

By enforcing strict policies that comply with local laws and follow well established guidelines, as well as training programs to ensure they are followed, ResilientIntellect's new branch can minimize the risk of a breach and quickly grow to a full sized functioning unit that local clientele can trust.

The impact to revenue and reputation caused by any serious incidents can also be minimized via careful contingency planning that accounts for the threats ResilientIntellect is likely to face, such as data poisoning or cloud service downtime. By laying down disaster recovery and business continuity plans, ResilientIntellect can ensure a smooth transition from

its reactive loss minimizing efforts back into regular business whilst recording incidents for future improvement and required legal reporting.

Should ResilientIntellect develop its EU unit with these facets in mind, it should be able to continue growing at a rapid pace.

bibliography

- [1] C. I. Torres and R. E. Crossler, "Promoting Security Behaviors in Remote Work Environments: Personal Values Shaping Information Security Policy Compliance," *Information Systems Research*, Jul. 2024, doi: <https://doi.org/10.1287/isre.2021.0563>.
- [2] Richik Maity and K. L. Lee, "The impact of remote and hybrid work models on small and Medium-sized enterprises productivity: a systematic literature review," *SN Business & Economics*, vol. 5, no. 10, Sep. 2025, doi: <https://doi.org/10.1007/s43546-025-00931-7>.
- [3] K. Shaw, "What is Zero Trust Network Architecture (ZTNA)?: Zero Trust is a security strategy (not a product) based on the idea that devices and users are considered untrusted until they can be authenticated," *Network World (Online)*, 2022. Available: <https://www.proquest.com/trade-journals/what-is-zero-trust-network-architecture-ztna/docview/2757077366/se-2>.
- [4] IT Governance, "ISO 27000 Series of Standards | IT Governance UK," *Itgovernance.co.uk*, 2016. <https://www.itgovernance.co.uk/iso27000-family> (accessed 16th Dec 2025)
- [5] Tejaswini C. Herath, Hemantha S. B. Herath, and John D'Arcy. 2020. Organizational Adoption of Information Security Solutions: An Integrative Lens Based on Innovation Adoption and the Technology- Organization- Environment Framework. *SIGMIS Database* 51, 2 (May 2020), 12–35. <https://doi.org/10.1145/3400043.3400046>
- [6] "What is SASE? | Secure access service edge," *Cloudflare.com*, 2024. <https://www.cloudflare.com/learning/access-management/what-is-sase/> (accessed 20th Dec 2025)
- [7] P. Katkar, R. Sheikh, CYBER HYGIENE: DEFENCE IN THE DIGITAL ERA, *International Research Journal of Modernization in Engineering Technology and Science*, (November 2025), e-ISSN: 2582-5208
- [8] M. E. Whitman and H. J. Mattord, *Principles of information security*, 7th ed. Boston, Mass.: Cengage Learning, 2022.
- [9] N. Komanduri and S. Sankaran, "Experimental Assessment of Wireless LANs against Rogue Access Points," *IEEE Xplore*, Dec. 01, 2021. <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9701078>

- [10] P. Ashok, S. L. Sridevi, R. Gorli, K. M. Krishna, S. Gopinath, and A. Verma, "Cybersecurity Risks in Remote Work: Safeguarding Distributed Networks and Endpoint Devices," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, pp. 1–6, Aug. 2025, doi: <https://doi.org/10.1109/worldsuas66815.2025.11199102>.
- [11] ukcybersecuritygrouppltd, "Your Secret Weapon: Integrating Honeypot Systems to Protect Critical Data," *UK Cyber Security Group Ltd*, Feb. 14, 2025. <https://www.ukcybersecurity.co.uk/blog/news-advice/your-secret-weapon-integrating-honeypot-systems-to-protect-critical-data/> (accessed 29 Dec 2025)
- [12] UK Government, "UK General Data Protection Regulation," *legislation.gov.uk*, 2018. <https://www.legislation.gov.uk/eur/2016/679/contents>(accessed 1st Jan 2026)
- [13] "Incident response planning covers the identification of, classification of, and response to an incident." Accessed: Jan. 05, 2026. [Online]. Available: https://www.idc-online.com/technical_references/pdfs/data_communications/Incident_Response_Planning.pdf (accessed 1st Jan 2026)
- [14] NIST, "Cybersecurity Framework," *National Institute of Standards and Technology*, 2025. <https://www.nist.gov/cyberframework> (accessed 1st Jan 2026)
- [15] H. Rama and Vishal Gudhka, "Secure and Scalable AI Pipelines for Network Automation in Highly Regulated SaaS Environments," pp. 96–99, Nov. 2025, doi: <https://doi.org/10.1109/cscloud66326.2025.00022>.
- [16] Microsoft, "What is SaaS? Software as a Service | Microsoft Azure," *azure.microsoft.com*, 2023. <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-saas>
- [17] EIOPA, "Digital Operational Resilience Act (DORA)," *www.eiopa.europa.eu*, 2025. https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en