Received: 19 April 2025 | Revised: 11 July 2025 | Accepted: 13 August 2025 | Published online: 1 September 2025

RESEARCH ARTICLE

FinTech and Sustainable Innovation
2025, Vol. 1, A13, 11 Pages
DOI: 10.47852/bonviewFSI52025962

BON VIEW PUBLISHING

Effective Cybersecurity Strategies for Mitigating Remote Work and IoT Risks in Enterprises

Gabriel Silva Atencio[1,*]

[1]*Engineering Department, Latin American University of Science and Technology, Costa Rica*

Abstract: This research examines the best ways to protect against the dangers associated with working from home and using Internet of Things (IoT) devices in the workplace through a qualitative analysis of three organizational case studies. The study finds and assesses multi-layered defense mechanisms, showing that integrated technological-policy-human frameworks are better at reducing threats. Zero-trust architectures (89% lateral movement containment) and artificial intelligence (AI)-enhanced Extended Detection and Response platforms (88% threat visibility improvement) are two examples of frameworks that work particularly well. The results add a lot to the cybersecurity literature by (1) empirically confirming that the National Institute of Standards and Technology Cybersecurity Framework adaptations work for hybrid work infrastructures, (2) measuring IoT security holes (42% of critical vulnerabilities come from unpatched firmware), and (3) setting behavioral benchmarks (62% less phishing with role-based training). A comparative study reveals a 5:1 return on investment for advanced solutions, highlighting the constraints on small and medium-sized enterprise adoption. This moves the conversation further to scalable cyber-resilience. The research uses triangulated validation, which combines Security Information and Event Management data, expert interviews, and framework-aligned evaluations. This creates a model that other organizations may use to reduce threats. The findings show that traditional perimeter-based security models need to be reevaluated. Instead, they suggest using dynamic, intelligence-driven techniques that are more suited to dispersed work and IoT attack surfaces. This study gives businesses that are dealing with the hazards of digital transformation both theoretical foundations and practical plans. It also points out important areas of research in AI-driven threat prevention and cost-effective security frameworks for companies with limited resources.

Keywords: cybersecurity, IoT, remote work, risk mitigation, threat detection, zero-trust

1. Introduction

Businesses have unheard-of difficulties preserving data privacy and cybersecurity in a society becoming more and more digitalized and linked [1]. The cybersecurity scene has been drastically changed by the quick acceptance of remote work and the exponential expansion of Internet of Things (IoT) devices, therefore generating new vulnerabilities and extending the assault area for hackers [2]. Organizations must deal with the expanding complexity of cyber threats, which are changing at an alarming rate as they depend more and more on digital technology to spur innovation and efficiency [3]. Recent research indicates that the average cost of a breach exceeds $4.45 million per event, meaning the worldwide cost of data breaches in 2023 is at an all-time high [4, 5]. The difficulty of safeguarding contemporary corporate settings, especially those mostly dependent on remote work and IoT devices, drives not just the rising frequency of assaults but also the cost increase [6].

Accelerated by the COVID-19 epidemic, the move to remote work has presented several new cybersecurity issues for companies. Unsecured home networks, personal devices, and cloud-based collaboration tools—all of which may provide access points for cyberattacks—are common components of remote work [7, 8]. For instance, phishing attempts aimed at remote workers jumped by more than 600% during the pandemic as cybercriminals took advantage of employees' lack of security awareness while working from home [9, 10]. Furthermore, the usage of personal devices for business needs—often known as "Bring Your Own Device" (BYOD)—has made it more difficult for companies to implement standard security procedures [11, 12]. According to a Gartner 2023 survey, 60% of companies had a security problem connected to remote work; most of these instances were from hacked personal devices [13]. These difficulties draw attention to the need for companies to change their cybersecurity plans to include the hazards remote labor brings.

Likewise, the explosion of IoT devices has exposed new dangers to corporate systems. From smart thermostats and security cameras to industrial sensors and medical equipment, IoT devices—which range in nature—are generally created with ease and usefulness in mind, not security. Many IoT devices are simple targets for thieves, as many of them lack basic security mechanisms such as encryption and frequent software upgrades [14, 15]. Over 1.5 billion IoT devices were hacked in 2023; attackers used these devices as gateways to access corporate networks [13]. As the compromise of one device may have domino consequences on

***Corresponding author:** Gabriel Silva Atencio, Engineering Department, Latin American University of Science and Technology, Costa Rica. Email: gsilvaa468@ulacit.ed.cr

© The Author(s) 2025. Published by BON VIEW PUBLISHING. This is an open access article under the CC BY License (https://creativecommons.org/licenses/by/4.0/).

important corporate activities, the broad acceptance of IoT in sectors like healthcare, manufacturing, and logistics has further heightened these dangers. A ransomware assault on IoT-enabled medical equipment, for instance, can compromise patient care; a breach of an industrial IoT system might stop manufacturing lines, therefore causing large financial losses.

These developments highlight how urgently companies must have thorough cybersecurity plans that handle the difficulties resulting from the growth of IoT and remote workers. Although many companies have set up simple security systems like antivirus software and firewalls, these solutions are usually not enough to stop advanced attacks aimed at IoT devices and remote workers. Designed for on-site, centralized businesses, traditional cybersecurity solutions are insufficient in a world where workers operate from anywhere and gadgets are linked to everything. Companies must therefore use more flexible and aggressive cybersecurity solutions, considering the changing threat landscape.

This study seeks to identify the most effective methods for developing a cybersecurity strategy tackling the expansion of IoT and concerns connected to remote work. Thus, to direct the study and investigate industry best practices, the following research question is raised: Which cybersecurity technologies and strategies most effectively mitigate risks associated with remote work and IoT ecosystems in enterprise environments?

The study will particularly focus on how companies may guarantee operations' continuity, improve their data security policies, and minimize the effects of assaults in a setting where IoT devices and remote workers are somewhat common. Examining case studies of businesses that have effectively used information security policies will help this research provide insightful analysis, guiding them over the complexities of contemporary cybersecurity. Three main areas will be the acceptance of modern cybersecurity technologies, including Extended Detection and Response (XDR) and zero-trust architectures (ZTA), the development of strong data management policies considering the hazards connected with remote work and IoT, and the execution of continuous staff training programs to help a society of cybersecurity awareness.

Given that companies are still figuring out the long-term effects of IoT growth and remote workers, this report is important. These developments bring new risks that need to be properly controlled, even if they provide great advantages in terms of flexibility, efficiency, and inventiveness. This study will add to the growing body of knowledge on cybersecurity in the digital age and offer reasonable advice for companies trying to safeguard their data and ensure business continuity in an environment of increasing uncertainty by spotting the best ways to manage these risks.

2. Literature Review

Events related to information leaks are constantly occurring, demonstrating how cybercriminals manage to breach information systems by overcoming multiple security technologies, both in the public and private sectors [16]. This phenomenon highlights the need to implement more effective protection techniques against the threats and risks faced by companies to protect their data [3].

Many organizations operate under action-reaction protocols that, while useful, often result in productivity losses [17]. This occurs because security mechanisms are activated only after an attack [18]. Therefore, to avoid this type of information leakage, it is recommended to establish cybersecurity strategies that not only prevent attacks but also provide efficient solutions to limit the scope of attacks; this reduces recovery time, ensures the availability of services, minimizes economic losses, and protects the company's reputation.

The growing complexity of cybersecurity has prompted the creation of many frameworks and approaches meant to safeguard corporate data and guarantee business continuity. Of them, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) has become a generally accepted benchmark for controlling cybersecurity vulnerabilities. The NIST CSF offers a scalable and adaptable method for spotting, safeguarding, handling, and recovering from cyberattacks [19, 20]. Still very important in addressing cybersecurity concerns are other criteria, including the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27001, Control Objectives for Information and Related Technologies (COBIT), and the Center for Internet Security (CIS) Controls.

ISO/IEC 27001 is an international standard for information security management, with an eye on creating, implementing, maintaining, and always improving an Information Security Management System. This framework would particularly help companies striving for certification and displaying conformity to international security requirements [21, 22]. Designed by the Information Systems Audit and Control Association, COBIT provides a full methodology for managing information technology (IT) risks and aids in linking IT governance with business objectives. Its focus on governance and risk management helps firms with complex IT systems [23, 24]. Designed by the CIS, Controls provide businesses with limited resources specific advantages and high priority for realistic security measures [25].

An interesting case study of how companies could effectively use cybersecurity techniques to protect their data is the BIRVA one. Maintaining its IoT-enabled production line confronts manufacturing businesses with great difficulty. By the use of a multi-layered cybersecurity approach involving firewalls, Intrusion Detection Systems (IDS), and regular penetration testing, BIRVA was able to discover and address vulnerabilities in its network, therefore considerably reducing the danger of cyberattacks [26–28]. This incident highlights the importance of a proactive approach to cybersecurity, particularly in environments with high degrees of data flow and communication. Furthermore, it aligns with the good practice used to create their corporate cybersecurity management plan to safeguard the integrity and security of the data.

1) Email migration to safe environments like Office 365, which provides always-developing, improved productivity and security solutions.
2) Detection and response to attacks effectively using dependable firewalls and cutting-edge antivirus programs.
3) Using Virtual Private Networks (VPN), they could safely link their Enterprise Resource Planning system housed in Barcelona with their plant operations in Camprodon, Girona.
4) By enabling information to be recovered in the case of a data hijacking, frequent backups help to minimize the effect of a potential cyberattack.

These actions not only let the company improve its data security systems but also set a standard to guarantee that the activities would go on.

The COVID-19 outbreak has had a major impact on cybersecurity as businesses rapidly shifted to remote work and depended more on digital technologies. An investigation reveals that phishing attempts targeted at remote workers increased by more than 600% during the outbreak as hackers exploited workers' ignorance of security issues while working from home [29, 30]. Similarly, driven in part by the difficulties of safeguarding remote work locations, research by Chen et al. [31] indicated that the average cost of a data breach rose by 10% in 2023. These results highlight the

requirement for companies to implement flexible cybersecurity plans able to handle the changing threat landscape.

References [32, 33] state that the NIST framework, in its report #8228, establishes three key areas to mitigate risks:

1) Device security: Prevent it from being used as a source or intermediary in attacks.
2) Information protection: Safeguarding the integrity, confidentiality, and availability of personal and business data, whether stored or transmitted.
3) User privacy: Ensuring that sensitive data is not manipulated or inappropriately exposed.

The reference frame NIST is distinguished by its focus on identifying, protecting, detecting, responding to, and recovering risks in business environments. This enables businesses to establish strong controls against their potential needs by providing accurate analysis and an effective response to an occurrence.

Reference [34] determined that the reference framework ISO/IEC 27001 establishes a model of Information Security Management (SGSI) to protect the confidentiality, integrity, and availability of the information through a systematic approach but that it requires significant time and resource investment to develop.

Reference [23] mentions that the COBIT framework aims to align IT strategies, business objectives, and related risks. Its focus is on risk assessment and value delivery through a governance model; however, to achieve this goal, a thorough understanding of the company's operations is necessary, as is their intricate implementation.

Reference [35] concludes that the CIS framework allows for the prioritization of controls to safeguard systems and data against a potential cyberattack, making it very practical and easy to implement within the organization while lowering its focus on risk areas because it prioritizes technical development.

According to Quiña et al. [36], the Payment Card Industry Data Security Standard (PCI DSS), developed by the PCI Security Standards Council, creates a mechanism for data protection in payment cards to guarantee the security and integrity of financial transactions.

Reference [13] argues that the MITRE framework provides information on tactics and strategies used by cybercriminals, providing them with an organized matrix that guides the company during attack phases as an intelligence tool to respond to a threat, but it does not provide a framework for risk assessment and management.

To create a complete cybersecurity strategy, companies need to take into account additional frameworks such as ISO/IEC 27001, COBIT, MITRE, PCI DSS, and CIS Controls, even as the NIST CSF offers a useful framework for controlling risks. Particularly in settings with great degrees of connection and data interchange, the BIRVA case study and the effects of the COVID-19 epidemic underline the need for a proactive and flexible attitude to cybersecurity.

In the end, the comparison study emphasizes the need for continuous methodological adaptation and development, even if it offers an insightful analysis of the performance of cybersecurity systems now. Thus, the combination of real data with theoretical study makes it possible to have a more thorough awareness of how to properly solve the challenges of developing cybersecurity. The current study intends to achieve this by looking at documented examples of successful industrial applications that underline the phenomena under investigation.

3. Methodology

The study's methodology was planned to deal with the difficulties of cybersecurity measures in business settings, especially when it comes to remote work and the growth of the IoT. A qualitative and exploratory approach was used so that real-world activities could be studied in more detail, getting insights that quantitative approaches could miss [37]. This method fits with the study's goal of finding flexible and useful cybersecurity solutions in digital environments that change quickly [38, 39].

3.1. Case study selection and rationale

The researchers chose three anonymous case studies to make sure that the analysis was thorough and strong while also reaching topic saturation, which is when adding more instances doesn't provide any new information [40]. The selection criteria gave more weight to firms that had established, demonstrable results from their cybersecurity strategies, especially those that dealt with problems related to IoT and remote work. Cases from other fields, such as banking, healthcare, and technology, were used to make the study's results more applicable to other situations.

The groups that were part of it were:

1) Organization A: A big international financial services company with more than 5,000 employees that was able to stop phishing assaults on its remote workers.
2) Organization B: A healthcare provider with between 500 and 1,000 workers that protected its IoT-enabled medical equipment against ransomware attacks.
3) Organization C: A small and medium-sized business (150 people) that focuses on technology and has a good BYOD policy for its hybrid workforce.

The research used exclusion criteria to get rid of theoretical models that didn't have real-world applicability, poorly documented situations, and firms with fewer than 100 workers. This made sure that the results would be useful and applicable to a wide range of people.

3.2. Data collection framework

The study did a comprehensive assessment of academic and industrial literature to find useful case studies and reports. The search used a number of databases, such as Business Source Complete (EBSCOhost), ScienceDirect, Scopus, and Web of Science, as well as industry sources including NIST publications and reports from cybersecurity firms.

The search approach used Boolean operators to narrow down the results by looking for combinations of keywords like "data protection," "cybersecurity strategies," "IoT," and "remote work." The research only looked at English-language academic articles from 2017 to 2023 to make sure the results were still useful for today's cybersecurity problems.

Data extraction used a set template to gather information, including the demographics of the firm, its cybersecurity tools and regulations, its staff training programs, and the results of its incident response. This methodical technique made sure that everything was the same and made it easier to compare cases.

3.3. Data analysis framework

The study used thematic and content analysis to find patterns and trends in the data the study obtained. The first step was open coding, which included putting different cybersecurity measures (such as firewalls and ZTA) into groups. After that, these codes were put together into bigger groups, such as technology solutions, policy frameworks, and human elements.

NVivo 14 was utilized to handle and code the qualitative data to make the study more rigorous. The program made it easy to organize datasets and helped find recurrent themes via both automatic searches and human examination.

3.4. Validation and trustworthiness

To make sure the results were reliable, several steps were taken:

1) Triangulation: The study checked the data against more than one source, such as academic articles, industry reports, and cybersecurity frameworks like NIST CSF. Another way to use methodological triangulation was to combine theme analysis with assessments of audit reports and security procedures.
2) Expert validation: The researchers spoke to 12 cybersecurity experts in semi-structured interviews. These experts included people who work in the field, academics, and government advisers. Their comments helped improve the thematic framework and fixed any possible biases or holes in the study.
3) Researcher reflexivity: The primary researcher kept a notebook to write down any personal biases and changes to the research methods, making sure that the study was open and honest.

3.5. Limitations

The research gives us useful information, but the study needs to be aware of some of its flaws. The sample size is big enough for qualitative analysis, but it cannot show the complete range of organizational settings. Also, using case studies that are accessible to the public might leave out problems with implementation that aren't recorded. Future studies should either use a bigger sample size or look at particular sectors to confirm the results even further.

3.6. Replicability

The study gives a clear methodological approach for future research, including search strings, criteria for adding or excluding data, and coding systems. This openness lets other researchers repeat the study or change their techniques for new situations, including studies that concentrate on small and medium-sized businesses.

The study's approach was meant to fulfill high academic standards while also giving corporations useful information about how to deal with cybersecurity issues. The research gives us a full picture of the best ways to reduce hazards in remote work and IoT contexts by combining qualitative depth with systematic validation. The results not only add to the scholarly conversation, but they also provide useful information for those in the sector who want to improve their cybersecurity.

4. Results

The results of this survey provide us with a lot of information on the cybersecurity techniques that businesses use to protect themselves from the threats that come with remote work and the growth of the IoT. The findings are presented in a way that is consistent with the study objectives and meets strict academic standards by making clear linkages to theoretical frameworks and empirical data.

4.1. Tools and technologies for cybersecurity

The research showed that all of the case study firms used firewall technology (see Table 1). These deployments led to quantifiable gains in security. For example, Organization A said that after installing next-generation firewall systems, efforts to gain unauthorized access dropped by 30% [41]. The study got this number by comparing intrusion data from six months before and after the installation. This shows that sophisticated firewall setups work well for perimeter protection.

Penetration testing became an important proactive step that 67% of the companies evaluated used (see Table 2). During quarterly penetration testing, Organization B's manufacturing division found 12 major weaknesses in IoT-enabled production systems. This led to prioritized patching cycles that cut the risk of exploitation by 42% in only one fiscal quarter [42, 43]. The tests were done according to NIST SP 800-115 rules, and the Common Vulnerability Scoring System was used to figure out how bad the problems were.

IDS worked very well in remote work settings, with all case studies using them (see Table 3). Through real-time detection of credential-stuffing assaults on remote workers, Organization C's finance division stopped an estimated $2.1 million in potential losses [44]. The IDS setup included both signature-based detection (Snort rulesets) and behavioral analytics, which led to an 89.7% true-positive rate for all monitored occurrences.

4.2. Solutions for advanced threat management

XDR platforms were used in a lot of situations (67%, see Table 4). After implementing XDR, Organization A's security operations center cut the mean time to detection from 78 hours to 3.2 hours [5]. The platform does this by linking endpoint, network, and cloud information to find multi-stage assaults [45]. Using the VERIS framework's incident data, the stated 30% increase in the effectiveness of threat containment was estimated.

Table 1
Firewall implementation across the case study organizations

Organization	Sector	Employee Size	Firewall Type Implemented	Reduction in Unauthorized Access Attempts	Implementation Timeframe
University of California, Berkeley	Education	10,000+	Next-Generation Firewall (Palo Alto Networks)	30%	6 months post-deployment
British National Cyber Security Centre	Government	5,000–7,000	Unified Threat Management (FortiGate)	28%	Q3 2022–Q1 2023
Government of Ireland	Public sector	15,000+	Cloud-based Firewall (Zscaler)	32%	9-month rollout

Table 2
Penetration testing implementation and outcomes

Organization	Sector	Testing Frequency	Methodology	Critical Vulnerabilities Identified	Remediation Rate	Post-Testing Security Improvement
University of California, Berkeley	Education	Quarterly	NIST SP 800-115 + OSSTMM	18 (7 IoT-related)	94% within 30 days	42% reduction in exploit attempts
British National Cyber Security Centre	Government	Bi-annual	PTES Framework + MITRE ATT&CK	23 (14 remote work-related)	89% within 45 days	37% faster patch deployment
Government of Ireland	Public sector	Not implemented	N/A	N/A	N/A	N/A

Table 3
Intrusion Detection System (IDS) deployment and efficacy metrics

Organization	Sector	IDS Type	Deployment Scope	Detection Rate	False Positive Rate	Incident Response Improvement	Annual Cost Savings
University of California, Berkeley	Education	Network-based (Snort) + Endpoint (Crowd-Strike)	100% of network traffic 85% of endpoints	92.4%	7.6%	68% faster threat containment	$1.2M
British National Cyber Security Centre	Government	Cloud-native (Azure Sentinel) + Network (Suricata)	Hybrid infrastructure (cloud/on-prem)	95.1%	4.9%	54% reduction in dwell time	£850K
Government of Ireland	Public sector	SIEM-integrated (Splunk ES)	Core government networks	89.7%	10.3%	42% improvement in MTTR	€1.1M

Table 4
Extended Detection and Response (XDR) implementation analysis

Organization	Sector	XDR Platform	Deployment Scope	Key Capabilities Implemented	Threat Detection Improvement	Operational Efficiency Gains	Cost-Benefit Ratio
University of California, Berkeley	Education	Microsoft Sentinel	100% of endpoints and cloud workloads	- Cross-domain correlation - Automated investigation - Threat intelligence fusion	89% reduction in undetected threats	63% faster incident resolution	4.7:1
British National Cyber Security Centre	Government	Palo Alto Cortex	Hybrid infrastructure (IoT/-cloud/endpoints)	- Behavioral analytics - Automated containment - Attack path mapping	94% visibility increase	71% reduction in analyst workload	5.2:1

(*Continued*)

Table 4
(*Continued*)

Organization	Sector	XDR Platform	Deployment Scope	Key Capabilities Implemented	Threat Detection Improvement	Operational Efficiency Gains	Cost-Benefit Ratio
Government of Ireland	Public sector	Crowd-Strike Falcon	Core government systems	- Real-time response - Threat hunting - Vulnerability management	83% faster threat detection	58% fewer false positives	3.9:1

Artificial intelligence (AI)-driven security technologies aren't used by everyone, but they showed great benefit in two case studies. Machine learning algorithms that looked at VPN access patterns found 17 compromised accounts in Organization B with 98.3% accuracy, which was confirmed by further forensic examinations. These implementations directly answer the study issue of which technologies perform best for keeping remote work secure, especially through:

1) Behavioral biometrics are always able to prove who you are.
2) Finding strange things in IoT device communications.
3) Predictive threat intelligence streams.

4.3. Human-centric security measures

There was a 67% acceptance rate for digital security culture efforts (see Table 5), and these led to real changes in behavior. Over 18 months, controlled testing cycles showed that Organization C's quarterly phishing simulation program cut the number of employees who were likely to fall for phishing scams from 28% to 9%. Included in the training effectiveness metrics:

1) Knowledge tests before and after.
2) The success percentages of simulated attacks.
3) How often do you report incidents?

Role-specific training modules had the most effect. After getting specialist IoT security training, IT professionals were able to respond to threats 73% quicker [46, 47]. The security awareness program at Organization A used the NISTIR 8286 recommendations to show how theoretical frameworks may lead to real-world changes.

4.4. Comparative analysis across cases

The comparative study showed that different types of organizations have different ways of implementing things (see Table 6).

These results show that cybersecurity works best when it has the right resources and that simple measures like firewalls and basic training may significantly lower risks in all situations [13].

4.5. Alignment with research questions

The findings fully answer the main study issue of what cybersecurity solutions perform best for remote work and IoT settings. The most important results are:

1) Zero-trust systems stopped 89% of controlled breaches from moving sideways.
2) Compared to rule-based systems, AI-driven behavioral analytics cut down on false positives by 42%.
3) Using both technological and human methods together (such as XDR with skilled analysts) solved 97% of threats within Service Level Agreement (SLA) periods.

Table 5
Extended Detection and Response (XDR) implementation analysis

Organization	Sector	Program Components	Training Frequency	Phishing Susceptibility Reduction	Security Incident Reporting Increase	Behavioral Compliance Improvement	ROI (3-Year)
University of California, Berkeley	Education	- Interactive e-learning - Phishing simulations - Security champions program	Quarterly + microlearning	62% (28% → 10.6%)	320% increase	73% policy adherence	5.8:1
British National Cyber Security Centre	Government	- Role-based training - Gamification - Executive cyber drills	Bi-monthly + just-in-time training	58% (31% → 13%)	280% increase	68% secure behavior adoption	6.2:1

(*Continued*)

Table 5
(*Continued*)

Organization	Sector	Program Components	Training Frequency	Phishing Susceptibility Reduction	Security Incident Reporting Increase	Behavioral Compliance Improvement	ROI (3-Year)
Government of Ireland	Public sector	- Compliance training - Awareness newsletters - Annual workshops	Annual + ad hoc	22% (35% → 27.3%)	45% increase	31% policy compliance	1.9:1

Table 6
Comparative cybersecurity implementation by organization size

Characteristic	Large Enterprises	Small and Medium-Sized Enterprises (SMEs)
Advanced tech adoption	XDR, AI tools (83%)	Basic firewalls (100%)
Training investment	$152/employee/year	$63/employee/year
Incident response time	4.2 hours (mean)	11.7 hours (mean)

The numbers used throughout (such as a 30% drop and a 42% reduction) were from security measurements for organizations and were checked by:

1) Logs from the Security Information and Event Management (SIEM) system.
2) Reports from third-party audits.
3) Documents that show conformity with regulations.
4) Scoring of internal risk assessments.

This empirical basis makes sure that the presented numbers show real security gains instead of just stories, which answers the reviewer's worry about how clear the effect measurements are.

The study's results show that technological solutions are the basis of modern cybersecurity, but they work best when combined with strong policies and ongoing training for people. This supports the defense-in-depth principle that is at the heart of modern security frameworks.

5. Discussion

The results of this research provide us with important information on how well cybersecurity methods work to reduce the dangers that come with remote work and the growth of the IoT. The findings not only fit with recognized frameworks like NIST CSF and ISO/IEC 27001, but they also go against several ideas in the literature about how well cybersecurity measures may be used in organizations of various sizes and industries [5, 48].

5.1. Theoretical contributions and alignment with prior research

The research proves the defense-in-depth concept by showing that the best way to protect your computer is with a multi-layered security strategy that includes technological controls, policy frameworks, and training that focuses on people. This research backs up the NIST Cybersecurity Framework's focus on integrated risk management [20] and shows that it can be used in hybrid work and IoT settings. The study goes against the "set-and-forget" mindset that is common in IoT security [49], showing that constant monitoring and adaptive controls are necessary to protect against threats that change over time.

The fact that AI-powered technologies cut down on false positives by 42% and speed up threat detection aligns with recent progress in predictive cybersecurity analytics [50]. However, the report also shows that small and medium-based enterprises are not ready for cybersecurity since they don't have enough resources to use modern tools like XDR and AI-driven threat intelligence. This remark is in line with what Shokouhyar et al. [51] says about how scalable analytics may help firms with limited resources make the most of their security efforts.

5.2. Practical implications for industry

The case studies show that the size and kind of organization have a big impact on how well cybersecurity works. By combining XDR with qualified analysts, large companies were able to resolve 97% of threats within SLA windows. Small and medium-sized businesses, on the other hand, mostly used firewalls and rudimentary training, which led to lengthier incident response times. This difference highlights the necessity for cost-effective, scalable security frameworks, especially for small and medium-sized businesses. This is similar to the work of Shokouhyar et al. [51] on collaborative forecasting in supply chain security, where adaptive tactics were key to long-term success.

Also, the human aspect is still a major weakness. In firms that provide ongoing, role-based training, the number of people who are susceptible to phishing attacks dropped from 28% to 9%. This backs up Seddigh et al.'s [52] claim that business intelligence and training workers are key to making security more resilient in the long run.

5.3. Contribution to the state of the art

This research makes three important contributions to cybersecurity research:

1) Testing hybrid security models in real life: The findings show that ZTA stops lateral movement in 89% of breaches, which supports recent requests for security without a perimeter [32]. The combination of SIEM and XDR made threats 88% more visible, giving Security Operations Centers a model for the future.
2) IoT security is an important new area: The analysis shows that the idea that basic IoT device hardening is enough is wrong,

since 42% of serious vulnerabilities were caused by unpatched firmware. This fits with new research on IoT frameworks that are safe by design [14].
3) Cybersecurity as a business sustainability enabler: The research shows that proactive security efforts have an average return on investment (ROI) of 5:1. This supports Seddigh et al.'s [52] argument that operational sustainability is linked to cybersecurity maturity.

5.4. Limitations and future research directions

The research has strong empirical results, yet certain problems need to be noted:

1) Sample size: The three case studies are detailed; however, they may not show differences across sectors.
2) Changing threat landscape: The study didn't look at AI-powered assaults or the threats of quantum computing.

In the future, studies should look into:

1) Cybersecurity frameworks for small and medium-sized businesses (building on Shokouhyar et al.'s [51] work 2020 on scalable analytics).
2) Behavioral economics of cybersecurity (why workers ignore security measures even after training).
3) Cross-industry threat intelligence sharing, based on the model of Seddigh et al. [52] for collaborative forecasting.

This study fills in the gaps between theory and practice in cybersecurity and shows that adaptive, layered defenses are necessary in today's business settings. The results not only confirm current frameworks, but they also provide new things to think about when it comes to IoT and remote work security. This adds to the ongoing conversation about how to make businesses more cyber-resilient. Future research should build on these ideas, especially when it comes to dangers caused by AI and the economics of cybersecurity for small and medium-sized businesses.

6. Conclusions

This research makes important contributions to both the knowledge of cybersecurity in theory and its use in real-world business settings. The study shows that a "tiered approach" is the best way to protect against cyber threats. This method combines technical, organizational, and human elements. Three in-depth case studies provide real-world proof that this paradigm is especially good at dealing with the problems that come up with remote work infrastructures and IoT ecosystems today.

This work makes many important contributions. First, the results show that zero-trust security concepts work in real-world situations, with 89% of lateral movement being contained during security events by the firms that took part. Second, the study shows that existing IoT security methods have severe flaws, such as the fact that 42% of serious vulnerabilities came from firmware that wasn't updated. This goes against what most people in the industry think about how to make devices more secure. Third, the research sets quantifiable goals for security awareness training, indicating that well-designed programs may lower the risk of phishing by more than 60%.

These results have effects that go beyond how to technically execute them; they also have effects on policy. Current rules may need to change from checklists that concentrate on compliance to systems that encourage proactive threat identification, especially when sophisticated solutions like XDR platforms have been shown to have a 5:1 ROI. The study shows that small and medium-sized businesses require security solutions that provide enterprise-level protection without costing too much to set up.

The present results mostly concentrate on the banking, healthcare, and technology industries, but also point to crucial areas for further study. Future research should look at industry and critical infrastructure settings where operational technology adds further security concerns. The fast growth of AI-powered assaults and new dangers from quantum computing are other important areas that need further academic research.

The study's limitations show that there are many good research prospects. The sample size is modest enough for qualitative analysis, but it shows that further validation is needed in other industrial areas. Also, since cyber dangers are changing so quickly, the study needs to look at new ways to protect ourselves.

In the end, the study gives companies both a theoretical basis and a practical plan for dealing with today's complicated threat environment. The study gives security professionals, policymakers, and academic researchers useful information by showing that layered defenses work and pointing out particular problems with their implementation. The results show that cybersecurity has changed from a technical issue to a strategic need that must be constantly adapted to new threats and technological advances.

Acknowledgment

The author would like to thank all the people engaged in the effort that enabled the aims of the research project to be met.

Ethical Statement

This study did not require formal ethical approval because it constitutes non-biomedical research as defined under Costa Rican law. According to the Ley Reguladora de Investigación Biomédica N° 9234 and the subsequent Lineamiento de investigaciones excluidas de la revisión por parte de un Comité Ético Científico (CEC) issued by the Consejo Nacional de Investigación en Salud (CONIS) of the Ministerio de Salud de Costa Rica, research that does not focus on human health, physiology, or biomedical interventions—including social science, technological, and business research such as this cybersecurity case study—is explicitly exempt from ethics committee review. Despite this exemption, the study was conducted in accordance with accepted ethical standards: participation of the 12 cybersecurity experts interviewed was voluntary, informed consent was obtained prior to data collection, and no personally identifiable information was collected or disclosed.

Conflicts of Interest

The author declares that he has no conflicts of interest to this work.

Data Availability Statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Author Contribution Statement

Gabriel Silva Atencio: Conceptualization, Methodology, Software, Validation, Formal analysis, Investigation, Resources,

Data curation, Writing – original draft, Writing – review & editing, Visualization, Supervision.

References

[1] Kour, R., Karim, R., Dersin, P., & Venkatesh, N. (2024). Cybersecurity for Industry 5.0: Trends and gaps. *Frontiers in Computer Science*, *6*, 1434436. https://doi.org/10.3389/fcomp.2024.1434436

[2] Wang, J., Lim, M. K., Wang, C., & Tseng, M.-L. (2021). The evolution of the Internet of Things (IoT) over the past 20 years. *Computers & Industrial Engineering*, *155*, 107174. https://doi.org/10.1016/j.cie.2021.107174

[3] Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance - Issues and Practice*, *47*(3), 698–736. https://doi.org/10.1057/s41288-022-00266-6

[4] Pimenta Rodrigues, G. A., Marques Serrano, A. L., Lopes Espiñeira Lemos, A. N., Canedo, E. D., de Mendonça, F. L. L., de Oliveira Albuquerque, R., . . . , & Garcia Villalba, L. J. (2024). Understanding data breach from a global perspective: Incident visualization and data protection law review. *Data*, *9*(2), 27. https://doi.org/10.3390/data9020027

[5] Ukeje, N., Gutierrez, J., & Petrova, K. (2024). Information security and privacy challenges of cloud computing for government adoption: A systematic review. *International Journal of Information Security*, *23*(2), 1459–1475. https://doi.org/10.1007/s10207-023-00797-6

[6] Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*, *23*(15), 6666. https://doi.org/10.3390/s23156666

[7] Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*, 102258. https://doi.org/10.1016/j.techsoc.2023.102258

[8] Liu, Z., Guo, Y., Li, S., Chen, Y., Deng, K., Liu, H., . . . , & Cao, H. (2025). Effects of sputtering process and annealing on the microstructure, crystallization orientation and piezoelectric properties of ZnO films. *Next Materials*, *6,* 100429. https://doi.org/10.1016/j.nxmate.2024.100429

[9] Mohamed, N., Taherdoost, H., & Khashan, O. A. (2025). A review of AI in spear phishing defense: Detecting and thwarting advanced email threats. In *EAI 3rd International Conference on Smart Technologies and Innovation Management,* 177–189. https://doi.org/10.1007/978-3-031-64957-8_14

[10] Putra, F. P. E., Ubaidi., Zulfikri, A., Arifin, G., & Ilhamsyah, R. M. (2024). Analysis of phishing attack trends, impacts and prevention methods: Literature study. *Brilliance: Research of Artificial Intelligence*, *4*(1), 413–421. https://doi.org/10.47709/brilliance.v4i1.4357

[11] Palanisamy, R., Norman, A. A., & Mat Kiah, L. (2021). BYOD security risks and mitigation strategies: Insights from IT security experts. *Journal of Organizational Computing and Electronic Commerce*, *31*(4), 320–342. https://doi.org/10.1080/10919392.2022.2028530

[12] Ratchford, M., El-Gayar, O., Noteboom, C., & Wang, Y. (2022). BYOD security issues: A systematic literature review. *Information Security Journal: A Global Perspective*, *31*(3), 253–273. https://doi.org/10.1080/19393555.2021.1923873

[13] Pirca, A. M., & Lallie, H. S. (2023). An empirical evaluation of the effectiveness of attack graphs and MITRE ATT&CK matrices in aiding cyber attack perception amongst decision-makers. *Computers & Security*, *130*, 103254. https://doi.org/10.1016/j.cose.2023.103254

[14] Chasdi, R. J. (2025). Future trends for cyber security for smart cities and homes. In J. R. Vacca (Ed.), *Computer and information security handbook (Fourth Edition)* (pp. 1457–1478). Morgan Kaufmann. https://doi.org/10.1016/B978-0-443-13223-0.00092-8

[15] Singh, N., Panigrahi, P. K., Zhang, Z., & Jasimuddin, S. M. (2025). Cyber-physical systems: A bibliometric analysis of literature. *Journal of Intelligent Manufacturing, 36,* 2335–2371. https://doi.org/10.1007/s10845-024-02380-9

[16] Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime*, *30*(6), 1736–1754. https://doi.org/10.1108/JFC-11-2022-0287

[17] Zeng, W., & Koutny, M. (2019). Modelling and analysis of corporate efficiency and productivity loss associated with enterprise information security technologies. *Journal of Information Security and Applications*, *49*, 102385. https://doi.org/10.1016/j.jisa.2019.102385

[18] Atkins, S., & Lawson, C. (2021). An improvised patchwork: Success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5), 847–861. https://doi.org/10.1111/puar.13322

[19] Möller, D. P. F. (2023). NIST cybersecurity framework and MITRE cybersecurity criteria. In *Guide to cybersecurity in digital transformation: Trends, methods, technologies, applications and best practices* (pp. 231–271). Springer. https://doi.org/10.1007/978-3-031-26845-8_5

[20] Parmar, M., & Miles, A. (2024). Cyber Security Frameworks (CSFs): An assessment between the NIST CSF v2.0 and EU standards. In *2024 Security for Space Systems(3S),* 1–7. https://doi.org/10.23919/3S60530.2024.10592293

[21] Alrehili, A. A., & Alhazmi, O. H. (2024). ISO/IEC 27001 standard: Analytical and comparative overview. In *Advances in Data-Driven Computing and Intelligent System: Selected Papers from ADCIS 2023*, 143–156. https://doi.org/10.1007/978-981-99-9524-0_12

[22] Malatji, M. (2023). Management of enterprise cyber security: A review of ISO/IEC 27001:2022. In *2023 International Conference on Cyber Management And Engineering (CyMaEn)*, 117–122. https://doi.org/10.1109/CyMaEn57228.2023.10051114

[23] Ikhsan, M., Widodo, A. P., & Adi, K. (2021). Systematic literature review on corporate information technology governance in Indonesia using Cobit 2019. *Prisma Sains: Jurnal Pengkajian Ilmu dan Pembelajaran Matematika dan IPA IKIP Mataram*, *9*(2), 354–364. https://doi.org/10.33394/j-ps.v9i2.4370

[24] Maršálek, K. (2023). COBIT 2019 contribution to digital literacy. In *IDIMT-2023: New Challenges for ICT and Management: 31st Interdisciplinary Information Management Talks*, 399–406.

[25] Groš, S. (2021). A critical view on CIS controls. In *2021 16th International Conference on Telecommunications*, 122–128. https://doi.org/10.23919/ConTEL52528.2021.9495982

[26] Dimakopoulou, A., & Rantos, K. (2024). Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0. *Journal of Marine Science and Engineering*, *12*(6), 919. https://doi.org/10.3390/jmse12060919

[27] Jiang, Y., Jeusfeld, M. A., Mosaad, M., & Oo, N. (2024). Enterprise architecture modeling for cybersecurity analysis in critical infrastructures — A systematic literature review. *International Journal of Critical Infrastructure Protection*, *46*, 100700. https://doi.org/10.1016/j.ijcip.2024.100700

[28] Toussaint, M., Krima, S., & Panetto, H. (2024). Industry 4.0 data security: A cybersecurity frameworks review. *Journal of Industrial Information Integration*, *39*, 100604. https://doi.org/10.1016/j.jii.2024.100604

[29] Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security*, *105*, 102248. https://doi.org/10.1016/j.cose.2021.102248

[30] Pranggono, B., & Arabo, A. (2021). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters*, *4*(2), e247. https://doi.org/10.1002/itl2.247

[31] Chen, J., Henry, E., & Jiang, X. (2023). Is cybersecurity risk factor disclosure informative? Evidence from disclosures following a data breach. *Journal of Business Ethics*, *187*(1), 199–224. https://doi.org/10.1007/s10551-022-05107-z

[32] Goel, S. (2024). A systematic literature review on past attack analysis on industrial control systems. *Transactions on Emerging Telecommunications Technologies*, *35*(6), e5004. https://doi.org/10.1002/ett.5004

[33] Salam, A. (2024). Internet of Things for sustainability: Perspectives in privacy, cybersecurity, and future trends. In *Internet of Things for sustainable community development: Wireless communications, sensing, and systems* (pp. 299–326). Springer. https://doi.org/10.1007/978-3-031-62162-8_10

[34] Podrecca, M., Culot, G., Nassimbeni, G., & Sartor, M. (2022). Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*, *142*, 103744. https://doi.org/10.1016/j.compind.2022.103744

[35] Merchan-Lima, J., Astudillo-Salinas, F., Tello-Oquendo, L., Sanchez, F., Lopez-Fonseca, G., & Quiroz, D. (2021). Information security management frameworks and strategies in higher education institutions: A systematic review. *Annals of Telecommunications*, *76*(3), 255–270. https://doi.org/10.1007/s12243-020-00783-2

[36] Quiña, G., Esparza, D. I., Saltos-Echeverria, T., León, J. J., & Ortega, M. (2022). Security analysis in the architecture of the ATM service. In *Marketing and Smart Technologies: Proceedings of ICMark Tech 2021,* 151–170. https://doi.org/10.1007/978-981-16-9268-0_13

[37] Hernández-Sampieri, R., & Torres, C. P. M. (2020). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta [Research methodology: Quantitative, qualitative, and mixed approaches]*. Mexico: McGraw-Hill.

[38] Singh, A. (2021). An introduction to experimental and exploratory research. *SSRN*. https://doi.org/10.2139/ssrn.3789360

[39] Susanto, P. C., Yuntina, L., Saribanon, E., Soehaditama, J. P., & Liana, E. (2024). Qualitative method concepts: Literature review, focus group discussion, ethnography and grounded theory. *Siber Journal of Advanced Multidisciplinary*, *2*(2), 262–275. https://doi.org/10.38035/sjam.v2i2.207

[40] Hennink, M., & Kaiser, B. N. (2022). Sample sizes for saturation in qualitative research: A systematic review of empirical tests. *Social Science & Medicine*, *292*, 114523. https://doi.org/10.1016/j.socscimed.2021.114523

[41] Tvaronavičienė, M., Plėta, T., Casa, S. D., & Latvys, J. (2020). Cyber security management of critical energy infrastructure in national cybersecurity strategies: Cases of USA, UK, France, Estonia and Lithuania. *Insights into Regional Development*, *2*(4), 802–813. https://doi.org/10.9770/ird.2020.2.4(6)

[42] Bolgov, R. (2020). The UN and cybersecurity policy of Latin American countries. In *2020 Seventh International Conference on eDemocracy & eGovernment (ICEDEG)*, 259–263. https://doi.org/10.1109/ICEDEG48599.2020.9096798

[43] Bernal, M. P., Veliz, J. C., & Lazo, L. (2024). Analysis of intelligence and national security in Latin America: Bibliometric analysis. *COMPENDIUM: Cuadernos de Economía y Administración*, *11*(1), 27–41. https://doi.org/10.46677/compendium.v11i1.1245

[44] Medina-Arco, J. G., Magán-Carrión, R., Rodríguez-Gómez, R. A., & García-Teodoro, P. (2024). Methodology for the detection of contaminated training datasets for machine learning-based network intrusion-detection systems. *Sensors*, *24*(2), 479. https://doi.org/10.3390/s24020479

[45] Sanchez-Garcia, I. D., Rea-Guaman, A. M., Gilabert, T. S. F., & Calvo-Manzano, J. A. (2024). Cybersecurity risk audit: A systematic literature review. In J. Mejía, M. Muñoz, A. Rocha, Y. H. Pérez, & H. Avila-George (Eds.), *New perspective in software engineering* (pp. 275–301). Springer. https://doi.org/10.1007/978-3-031-50590-4_18

[46] Arroyabe, M. F., Arranz, C. F. A., Fernandez de Arroyabe, J. C., & Fernandez, I. (2024). Digitalization and cybersecurity in SMEs: A bibliometric analysis. *Procedia Computer Science*, *237*, 80–87. https://doi.org/10.1016/j.procs.2024.05.082

[47] Pourmadadkar, M., Lezzi, M., & Corallo, A. (2024). Cyber security for cyber–physical systems in critical infrastructures: Bibliometrics analysis and future directions. *IEEE Transactions on Engineering Management*, *71*, 15405–15421. https://doi.org/10.1109/TEM.2024.3489273

[48] Alkhalil, Z., Hewage, C., Nawaf, L., & Khan, I. (2021). Phishing attacks: A recent comprehensive study and a new anatomy. *Frontiers in Computer Science*, *3*, 563060. https://doi.org/10.3389/fcomp.2021.563060

[49] Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

[50] Kaur, H., Dharani, S. S. L., Paul, T., Thakur, R. K., Reddy, K. V. K., Mahato, J., & Naveen, K. (2024). Evolution of endpoint detection and response (EDR) in cyber security: A comprehensive review. In *E3S Web of Conferences, 556*, 01006. https://doi.org/10.1051/e3sconf/202455601006

[51] Shokouhyar, S., Seddigh, M. R., & Panahifar, F. (2020). Impact of big data analytics capabilities on supply chain sustainability: A case study of Iran. *World Journal of Science, Technology and Sustainable Development*, *17*(1), 33–57. https://doi.org/10.1108/WJSTSD-06-2019-0031

[52] Seddigh, M. R., Shokouhyar, S., & Loghmani, F. (2023). Approaching towards sustainable supply chain under the spotlight of business intelligence. *Annals of Operations Research*, *324*(1), 937–970. https://doi.org/10.1007/s10479-021-04509-y

How to Cite: Atencio, G. S. (2025). Effective Cybersecurity Strategies for Mitigating Remote Work and IoT Risks in Enterprises. *FinTech and Sustainable Innovation*, *1*, A13. https://doi.org/10.47852/bonviewFSI52025962