LOGPOINT

The business value of cybersecurity

Growing business securely

www.logpoint.com

EXECUTIVE SUMMARY

This whitepaper offers insights for C-level executives and board members on cybersecurity risk and how Cybersecurity investments can be measured into business value. It aims to inspire top management to discuss how to manage cybersecurity risk, what questions to ask the cybersecurity department, and help to understand how Cybersecurity can enable growth. It also includes examples of how Logpoint cybersecurity technology contributes to improved performance and how organizations use Logpoint to secure growth. The whitepaper could also be useful for CISOs and CIOs making a case for cybersecurity investments.

TABLE OF CONTENT

GROWING BUSINESS SECURELY WITH LOGPOINT

As cyber threat actors continue the barrage of cyberattacks against organizations of all shapes and sizes, cyber risk has caught attention outside of the cybersecurity domain. In particular, C-suite and board members are trying to understand whether their organization is safeguarded well enough to minimize the business impact of an attack and avoid non-compliance consequences and damage to the company's reputation.

All organizations have digital assets such as company secrets, confidential information, and customer data that are essential to protect. Cyberattacks and non-compliance could have detrimental consequences for the business and can leave organizations in a competitive decline. However, many executives struggle to understand precisely how cyber threats impact the company's risk profile and still perceive Cybersecurity as an outlier cost.

Striking the right balance between cyber risk management and cybersecurity investments is tricky. The C-suite often lacks the tools to understand cyber risk sufficiently, and cybersecurity departments are notorious for struggling to translate cyber risk into business risk. The result is a mismatch between risk profile and cybersecurity posture, leaving the business unprepared and missing the opportunity to use Cybersecurity to bolster performance and drive growth.

This whitepaper offers insights for executives and board members on cybersecurity risk and how Cybersecurity can enable secure business growth. It aims to inspire top management to discuss how to manage cybersecurity risk, what questions to ask the cybersecurity department, and help to understand how Cybersecurity can enable growth.

Cybersecurity can enable businesses to achieve the goals at the top of the agenda for executive management, like growth, business agility, risk reduction, and compliance. Logpoint's converged cybersecurity platform, combining sophisticated technologies, is central to a robust cybersecurity setup that works to close organizational gaps between executive and security leaders, bolster Cybersecurity, and provide the necessary capabilities to grow the business securely.

WHY CYBERSECURITY IS IMPORTANT

C-level executives and board members should be conscious of the cybersecurity threat and make investments in line with protecting the bottom line no matter the size of the company. That is as true for small and midsize companies as it is for large enterprises and publicly traded companies. According to **Verizon's 2021 Data Breach Investigations Report**, the difference in how many breaches small businesses and large enterprises face is insignificant.

Cyberattacks can be very costly. The world's leading cybersecurity economy researcher **Cybersecurity Ventures, expects global cybercrime costs to grow by 15 percent per year** over the next five years, reaching $10,5 Bn annually by 2025. If cybercrime were measured as a country, that would be the world's third-largest economy after the **U.S. and China.**

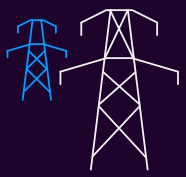
Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, and post-attack disruption to the normal course of business. It also includes forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

According to the recognized "Cost of a Data Breach" report by Ponemon Institute, the average cost of a single cyberattack is high and rises yearly. In 2019, the global average cost of a data breach was $3.86 million. In 2020, it rose to $4.24 million. In 2021, it was at an all-time high of $4.34 million.

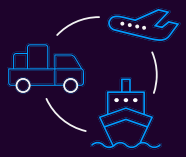
The cost of Cyberattacks reported by publicly traded companies

ISS
Facility Management
February 2020 Ryuk
Ransomware attack
Cost: **DKK 450-800m**

William Demant
Hearing Aid
September 2019 undisclosed
Malware attack
Cost: **DKK 550-650m**



Norsk Hydro
Aluminum
March 2019 LockaGoga
Ransomware attack
Cost: **NOK 650-750m**



Maersk
Shipping
June 2017 NotPetya
Ransomware attack
Cost: **USD 200-300m**

The actual cost of cyberattacks is hard to determine, as corporate victims of cybercrime often keep a tight lid on incidents. But occasionally, **publicly traded companies are forced to disclose the cost of cyberattacks in their annual reports**, proving that cyberattacks take a healthy cut of annual profits to the tune of hundreds of millions of dollars.

Cyberattacks on organizations come from a wide variety of threat actors ranging from disgruntled employees to foreign intelligence services and organized crime. Understanding the threat landscape, the motives, and the techniques employed by attackers is vital to comprehend the cybersecurity risk and the controls required to combat it.

Threat actors

- Insiders: Employees or business associates engaging in fraudulent activity or security breaches that harm the organization – knowingly or unknowingly.
- State-sponsored: A private actor conducting malicious activity on behalf of a state and thus has the means to deploy sophisticated attacks.
- Organized crime: Well-organized criminal groups combining skills to engage in malicious activities, such as ransomware.
- Hacktivists: An activist spreading an ideology through hacking and is often not motivated by malicious intent.
- Hacker: An individual tinkering with computers and networks and using the skills to overcome a technical problem – often associated with gaining unauthorized access.

Motives and techniques

- Script kiddie: An unskilled individual using existing and a well-known technique, program, or script to exploit weaknesses in devices
- Espionage: An unauthorized user gain access to sensitive or confidential data for financial, competitive, or political gain.
- Living off the land: Intruders gain access through legitimate software, leaving no evidence behind, to achieve their malicious objectives.
- Drive-bys: Hackers leverage security flaws in websites to launch automatic downloads of malicious software on the victim's device to steal information or damage data.
- Activism/hacktivism: Activists use various hacking tools to promote a political, religious, or moral agenda.
- Monetary gains (ransomware): Threat actors use ransomware to achieve substantial monetary gain, leaving the victim with financial and other collateral damage
- Destruction: Attackers launch attacks to destroy or damage data or physical objects or to sabotage, retaliate, or signal.

WHY CYBERSECURITY SHOULD BE PART OF YOUR BUSINESS STRATEGY

The ISO 31000 standard defines risk as "the effect of uncertainty on objectives." The key driver for risk management is to create and protect business value by assessing the company's ability to run business operations. Risk management aims to highlight and monitor risk, prevent risk materialization, and mitigate the consequences of a risk incident.

There are many ways of defining and categorizing the risks that organizations are facing today, but the various frameworks are generally very similar and aim to identify and manage operational risk. One of the best-known models for categorizing risk is defined in the Basel II guidelines by the Basel Committee on Banking Supervision.

The seven risk categories defined here are well-known to many C-level executives and board members:

Basel II risk categories

1. Internal Fraud
2. External Fraud
3. Employment Practices and Workplace Safety
4. Clients, Products, and Business Practice
5. Damage to Physical Assets
6. Business Disruption and Systems Failures
7. Execution, Delivery, and Process Management

A common denominator across risk categories

As most organizations have initiated a digital transformation in the past decade, almost all business-critical processes are at risk of cyberattacks.

The dependency on digital infrastructures is a unique common denominator across the Basel II risk categories, making Cybersecurity a foundational and critical factor to the operational risk of any organization.

Although executives acknowledge Cybersecurity as an important part of IT planning, they misunderstand the strategic character of cyberattacks, both as a severe threat to earnings and operations and as an opportunity. Organizational resilience to cyberattacks requires a fundamental change of mindset:
Executives must view Cybersecurity as strategic rather than operational and an opportunity rather than an expense.
A mature cybersecurity strategy provides a basis for securing critical assets and business processes, enhancing organizational learning, and noticing and capturing new strategic opportunities. It can reveal new strengths and fundamental weaknesses in leadership teams and organizational capabilities. It can pave the way to a fully digital business model or help create a new value proposition around security for customers.

Many executives fail to elevate the risk of cyberattacks to a strategic consideration because they mischaracterize the threat as a random, unpredictable event — when, in fact, no organization is immune, and cyberattacks are predictable surprises that exploit weaknesses in organizational strategies and capabilities. Some companies are more attractive targets than others, but cybercriminals directly attack organizations of all kinds and sizes.

UNDERSTANDING THE RISK: THE DISCUSSION ANY BOARD SHOULD HAVE

Based on the studies of organizations impacted **by the global 2017 NotPeteya attack**, Manuel Hepfer and Thomas C. Powell from Saïd Business School at the University of Oxford developed the model "Four Elements of Organizational Resilience to Cyberattack" to evaluate and improve organizational resilience to cyberattacks.

Each of the four elements of the model raises questions that executives can use to lead discussions on the company's approach to a cybersecurity strategy. Although some of these discussions are concerned with events after a cyberattack, all the discussions should happen now, as part of strategic planning before a cyberattack.

Four Elements of Organizational Resilience to Cyberattack

Before a cyberattack

Protecting the business

- What are our fundamental business processes?
- How vulnerable are they to cyberattacks?
- What are we doing to protect ourselves?
- How can we design our business processes to minimize our vulnerability to attack?
- What internal capabilities do we have for protecting against cyberattacks?
- Where are the strategic opportunities for improving cyber protection?

Broadening awareness

- How significant is the threat of cyberattack?
- Where is it most likely to come from?
- What form might it take?
- How are cyberattacks evolving?
- What capabilities do we have for detecting external threats?
- Where are the strategic opportunities for improving cyber-awareness?

After a cyberattack

Responding and recovering

- What capabilities do we have for responding to a cyberattack?
- What weaknesses would hinder our responsiveness?
- What can we do now to improve our responsiveness to an attack?
- What is our plan for business continuity in case of a cyberattack?
- How do we build an organizational structure that is dynamic enough to respond to different types of attacks?
- Who should be part of our crisis management team?
- What new strategic opportunities might be created if we improved our capabilities for cyber-responsiveness?

Managing consequences

- How would our key stakeholders respond if we were attacked?
- How would our customers be affected?
- How would financial markets respond?
- What can we do now to anticipate or shape these responses?
- What capabilities do we have for anticipating how stakeholders might respond?
- What are the strategic opportunities for managing the consequences of a cyberattack?

MANAGING THE RISK: 13 QUESTIONS TO ASK YOUR CYBERSECURITY DEPARTMENT

To manage cybersecurity risk, executive decisionmakers need to understand what risk scenario or incident looks like, how likely it is to occur, and what the consequences are. In addition, they should understand the residual risks, which is the risk remaining after the security measures have been applied. Understanding the risks allows for:

- Better decision-making in terms of security and supervisory controls
- Mitigation of the threat and better outcomes in case of a breach or attack
- Greater confidence in compliance with rules and regulations

Only by understanding the risk can organizations eliminate or mitigate the risk through appropriate cybersecurity controls and gain confidence that the most critical assets are sufficiently protected. Cybersecurity controls directly influence the likelihood and impact of cyberattacks and non-compliance incidents. C-level executives should familiarize themselves with the basic controls for Cybersecurity and compliance to better understand what the cybersecurity department is doing to keep the business safe.

Supervisory controls

Technical controls	Preventive controls	Reactive controls
The technical controls are the hardware and software components in place to protect the system. Examples of technical controls are: • Multi-Factor Authentication (MFA) • Encryption • Perimeter defenses • Test and production – system segregation • Security platforms (EDR, NDR, XDR, SIEM, etc.)	Preventive controls are in place to minimize the likelihood of an attack or a non-compliance incident. Examples of preventive controls are: • Cyber strategy • Cyber risk management • System monitoring • IT protection (firewalls, security incident management, endpoint protection, etc.) • Contractual obligations	Reactive controls exist to mitigate the impact of a cyber-attack. Examples of reactive controls are: • Cyber insurance • Backup and restore capabilities • Security incident response • Organizational preparation • Cancellation of orders • Public relations • Capital preparedness

Remember reactive controls and capital preparedness

Often, the executive level is satisfied knowing that the organization has technical and preventive controls to match the risk profile, but reactive controls are just as important. A key element among those and often overlooked is Capital preparedness.

The executive level needs to understand the cost of delay and no service and the recovery plan. They must ensure the business has the capital necessary to recreate functions and work. Otherwise, the company risks losing significant strategic effort and investments, resulting in competitive drawbacks.

For almost 20 years, Jan Quach, Logpoint's Global Director of Customers Success Engineering has been responsible for reassuring C-level executives and boards that Cybersecurity was robust. As a CISO-level cybersecurity executive in consulting, finance and manufacturing, Quach has worked tirelessly to raise executive awareness of the cybersecurity threat.

This is his checklist for the C-level executives and board members, including the questions that should be asked and answered by the cybersecurity leaders of any organization.

#	13 questions you should ask your Cybersecurity department	Asked/Answered?
1	How are operational risks addressed?	
2	What is the risk model?	
3	How are risks monitored and reported?	
4	How are risk scenarios identified?	
5	What are the top 10 risk scenarios identified and why?	
6	How does the scenario impact the business strategy?	
7	How are the consequences tiered, from partly to fully materialized risk scenario?	
8	What supervisory controls are in place?	
9	What reactive controls are in place?	
10	How were the controls selected?	
11	How are the controls tested to ensure efficiency?	
12	In the case of a materialized risk scenario, what is set aside for capital preparedness?	
13	What is the investigation model?	

Insisting on getting the answers to these questions allows the executive level to understand the business risk of cyberattacks, how well-protected the organization is, and how well-prepared it is when a cyberattack occurs – because it will. As the C-suite is responsible for ensuring business continuity, cyber risk and security should be central to their strategic considerations.

The C-suite and board should approach Cybersecurity holistically and understand how cyber threats can impact business and how the cybersecurity strategy supports the business strategy. They must acknowledge their responsibility in establishing necessary risk management and supervisory controls and ensure the company has responsible capital resources available in case of an incident. It's just good business.

DRIVING BUSINESS VALUE WITH CYBERSECURITY TECHNOLOGY

While many executives have realized that the cyber threat is real, only a few have realized how Cybersecurity can contribute to efficiencies and increased profit. In their study of the 2017 NotPeteya attack, Manuel Hepfer and Thomas C. Powell concluded that Cybersecurity could become a strategic asset by securing critical assets and business processes, enhancing organizational learning, and capturing new strategic opportunities, all contributing to improved competitive advantages.

A strong cybersecurity strategy enables organizations to transform Cybersecurity from a cost center to a profit center, by strengthening the brand, reducing cost, and increasing speed while contributing to optimizing processes and ensuring compliance. This provides tangible business value to the organization and supports business growth goals.

Brand	Cost	Speed	Optimization	Compliance
Strengthening brand and credibility with customers and partners	Reducing internal costs	Increasing operational speed	Exposing weaknesses and optimizing business processes	Ensuring compliance with rules and regulations

Mastering security data

The most critical key to efficient Cybersecurity is: Reliable data. Real-time data. Historical data. Organizations need all of it to mount an effective defense against external and internal threats. A holistic approach to cybersecurity contextualizes the data across the entire IT landscape, which gives the data meaning and empowers secure business growth.

Logpoint pulls all cybersecurity data together, verifies it, provides context, simplifies it, and prioritizes it based on urgency, history, damage already incurred, potential damage, and many other factors.

To master the security data and mount an effective cyber defense, Logpoint harnesses four key cybersecurity technologies in its unique Converged SIEM solution: SIEM, UEBA, SOAR, and Business-Critical Security (BCS) for SAP.

SIEM collects and analyzes security incidents in real-time, while UEBA uses AI technology to detect abnormal and risky behaviors. SOAR automates incident detection and response, and BCS for SAP automatically correlates and analyzes data from the cybersecurity infrastructure with data from business-critical systems, pertaining to SAP systems and applications, to provide unparalleled visibility.

Logpoint Converged SIEM accelerates threat detection, investigation and response. It allows organizations to achieve efficiencies of scale and consolidate the technologies used in their cybersecurity operations, making their security operations simple, efficient, and more effective than they ever thought possible.

The SaaS platform enables you to keep up to date with the latest threats with ready-to-use security content and playbooks. The C-suite can rest assured that the business is automatically protected against the most recent threats. In addition, the scalability and flexibility of SaaS allows businesses to use advanced analytics while maintaining control of financial requirements.

Security Information Event Management

Analyzing security incidents

- Centralize data monitoring
- Accelerate threat detection and investigation
- Out-of-the-box compliance support

Security Orchestration, Automation and Response

Automatic incident detection and response

- Reduce a cybersecurity risk
- Increase security operations efficiency
- Improve cyber intelligence

User and Entity Behavior Analytics

Detect unknown and insider threats using AI/ML technology

- Immediately spot insider threats
- Evaluate and assign risk
- Make SIEM and SOAR smarter

Business-Critical Security for SAP

Unparalleled application security for:

- Visibility across SAP
- Industry-leading analytics
- Integrate with existing security stack

The combination of tools enables a comprehensive data-driven approach to cybersecurity strategy and implementation. When cybersecurity metrics and data are easy to digest and stay above the technical fray, cybersecurity departments can engage in much more productive conversations, providing actual Business Value to the organization.

5 examples of Cybersecurity Business Value by Logpoint Converged SIEM

What?	How?	Business value
Reduce Risk from Phishing	By leveraging SOAR playbooks and the data in the SIEM from endpoints, email, network, and end users' direct input, the organization can run an automated playbook quickly, confirming emails are legitimate or cleaning them up from all users' mailboxes and machines automatically and quickly. Users become more likely to report suspicious emails, and time to remediation and resulting exposure is reduced considerably.	The organization significantly reduces the risk of attackers breaching it through phishing by engaging end users and responding quickly and automatically to concerns without increasing team costs.
Accurately Assign Resources by leveraging Threat Intelligence.	By leveraging SOAR playbooks to process and operationalize threat intelligence feeds, resources can be focused on battling the most likely threats.	Using industry specific Threat Intelligence allows organizations to focus their resources and efforts on known attack vectors, achieving cost-efficient response and risk reduction.
Reduce Cloud Risk	By melding the data from on-premises detection with data from cloud detection and running playbooks to automatically triage it, Cloud Risks are quickly exposed and remediated.	Allow the organization greater agility and acceleration of its cloud migration by reducing cloud risks for the organization.
Reduce Internal Threat Risk	By aggregating data from various user actions and Identity systems Logpoint can help detect malicious insider actions, flag and block them.	Organizations are often blind to insider risks. By monitoring and detecting potentially malicious actions, the risk is reduced.
Ransomware Response	By performing detection of known groups using ransomware to target organizations, as well as by automating the hunting of new threats and automating the recovery process, both the chance of occurrence and its impact are greatly reduced.	Organizations are at risk from Ransomware attacks. By both detecting and blocking such attacks early as well as recovering quickly after the attack, risk and its cost are greatly reduced.

CONCLUSION

Cybersecurity is the foundation of securing the growth of any business. It improves efficiency and reduces risk. As such, the C-suite needs to engage properly to ensure that cybersecurity is done right and works optimally for the business.

By analyzing security incidents, automating incident detection and response, and detecting unknown and insider threats, Logpoint enables organizations to centralize data monitoring, reduce and evaluate cyber risk, and increase security operations efficiency. In short, Logpoint is an essential cybersecurity platform that enables the Cybersecurity department to answer the C-suites questions and give them confidence that the business is growing securely.

Contact Logpoint

If you have any questions or want to learn more about Logpoint and how we can enable your business to grow securely, reach out to us at **sales@logpoint.com**.

PROVIDING BUSINESS VALUE WITH LOGPOINT

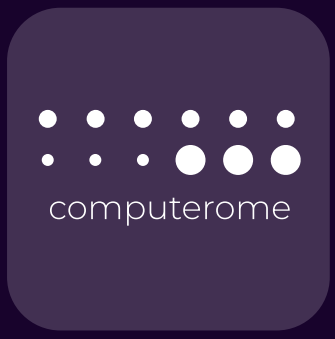
Logpoint boosts secure growth for organizations across the globe, from higher education, healthcare, and local government to manufacturing, services, and finance industries. Below 10 Logpoint customers have shared their real-life cases, illustrating how Logpoint technologies have helped them gain improved performance.

Danish National Life Science Supercomputing Center: Ensuring regulatory compliance

Computerome, The Danish National Life Science Supercomputing Center, is a High-Performance Computing facility specialized for Life Science.

Logpoint provides Business Value to Computerrome by:

1. Detecting unusual behavior
2. Ensuring regulatory compliance
3. Providing enhanced security for vast amounts of sensitive data



"Logpoint allows Computerome administrators to quickly detect unusual behavior in the system and to prevent misuse and data breaches. It provides that extra layer of security on top of the established security controls, which is required when handling vast amounts of data. It also allows us to provide our users with full insight and transparency"

Peter Løngreen

Director, Danish National Life Science Supercomputing Center.

Deutscher Alpenverein: Ensuring GDPR compliance across one million members

More than one million alpinists and mountain fans are organized in 356 regional associations, under the Deutscher Alpenverein (German Alpine Club) established in 1869.

Logpoint provides Business Value to Deutscher Alpenverein by:

1. Ensuring GDPR compliance across one million members
2. Providing a complete, failure-resistant, tamper proof and audit-ready storage of all log data
3. Reducing the number of false positives remarkably

"We were able to reduce the number of false positives remarkably, and a glance of a dashboard we now know what is happening in our entire IT infrastructure. This ultimately provides us with reassurance, that we are able to better assess the security situation at any given point in time"

Klaus Vogler

IT Manager, Deutscher Alpenverein.

Groupe Matmut: Providing 80-90% time savings in incident diagnostics

French insurance company Groupe Matmut, originally established in Rouen in 1961 as Mutuelle des Travailleurs Mutualistes, is major player in the French insurance market.

Logpoint provides Business Value to Groupe Matmut by:

1. Identifying new threat indicators
2. Providing 80-90% time savings in incident diagnostics
3. Allowing to upgrade the quality of service for the entire organization

"The savings generated by the Logpoint solution allowed us to upgrade the quality of service offered to our organization, which is an unexpected but much-welcomed benefit"

Cédric Chevrel

CISO, Groupe Matmut

Rémy Cointreau: Ensuring visibility across silos in the organization

Rémy Cointreau is a French luxury spirits provider with origins dating back to 1724. The current group, formed by the 1990 merger between E. Rémy Martin & Cie and Cointreau & Cie listed on the NYSE Euronext in Paris.

Logpoint provides Business Value to Rémy Cointreau by:

1. Ensuring visibility across silos in the organization
2. Delivered as a Managed Service
3. Pricing based on nodes rather than data volume ensuring predictable cost

"Billing is based on the number of nodes and not on data volume is important when using Endpoint Detection and Response. EDR can suddenly generate large numbers of logs. We had to match our budget to our needs, without any unpleasant surprises"

Xavier Leschaeve

CISO, Rémy Cointreau

PXP Solutions: Providing a granular view of threats including important context

With a history spanning 30 years, UK-based PXP Solutions has expanded from a predominant focus on the hospitality industry to providing payment processing solutions that meet the needs of merchants across multiple industry sectors and locations.

Logpoint provides Business Value to PXP Solutions by:

1. Ensuring PCI compliance
2. Providing a granular view of threats including important context
3. No extra cost as PXP business expands

"As a financial services company in a highly regulated industry, it is imperative that we maintain a strong security posture at all times. Whilst the investment in a SIEM solution was always driven by our need for a robust security infrastructure, we are also faced with a wide range of industry standards such as the PCI-DSS, GDPR, SOC 2, and the Point-to-Point Encryption standard, where non-compliance can mean the loss of customers. By using Logpoint we can keep a very granular view of our logs and easily identify any out-of-the-ordinary activity"

Graeme Zwart

CISO, PXP Solutions.

Family Building Society: Cutting response time to cyberthreats in half

UK-based Family Building Society provides mortgage products and services designed to enable family members to provide mutual assistance for capital projects while safeguarding their savings.

Logpoint provides Business Value to Family Building Society by:

1. Cutting response time to cyberthreats in half
2. Providing 70-80% savings on administrator resources spent on log analysis
3. SIEM solution at a predictable cost

"We now think of Logpoint as a member of the IT Security team. It provides immediate answers to a lot of questions that we would have struggled to answer under a more manual system. We can take logs from everywhere that they need to be gathered and collate and analyse as much as we need and the process of ingesting data is very open"

Andrew Ballard

Head of Technical Design & Delivery, Family Building Society

Scildon: Mitigating risk in a complex IT environment

Scildon is a Dutch Life- and Pension Insurance company. Originally founded in 1984 as Legal & General Nederland, the company was renamed Scildon in 2017 when it was acquired by the UK-based Chesnara-group, that owns life and pension companies in the UK, Sweden, and the Netherlands.

Logpoint provides Business Value to Scildon by:

1. Providing flexible and efficient security analytics
2. Mitigating risk in a complex IT environment
3. Saving 75% on IT administrators' resources

"Previously we would take turns spending hours analyzing the logs of the previous day. It was a dreadful and time-consuming task, often including conversion of data to other formats and split-screen work for manual correlation between log sources. Today everything is nicely served up, and if anything is missing, I'll just take 15 min to create a dashboard that will tell me what I need. A 50% reduction was the target, but in reality, it's more like 75%"

Alistair Kirkman

Security Manager, Scildon

Strata Service Solutions: Improving operational efficiency

Strata Service Solutions Ltd., based across three sites in the Southwest of England, is a unique organization. It focuses on delivering transformational IT Services into three local authorities, East Devon District Council, Exeter City Council, and Teignbridge District Council, while aiming to reduce costs, reduce risk and deliver the capability to support change.

Logpoint provides Business Value to Strata Service Solutions by:

1. Providing increased security
2. Improving operational efficiency
3. Comes at a Predictable cost

"Over the last 3 1/2 years, our use of Logpoint has grown considerably. We do not see it as a point product, but a solution that has grown with our business. And the fact that it is not only deployed for security makes it all the more valuable. Over the last few years, we have cut the number of IT suppliers from 400 to 190, so we are heavily invested with the organizations we have chosen to partner with. Logpoint is with us for the long run"

Laurence Whitlock

IT Director, Strata Service Solutions

Lancaster University: Enables 80-90% quicker response to cyberthreats

Lancaster University ranks consistently among the top 10 universities in the United Kingdom and is a renowned international institution, named International University of the Year in 2020.

Logpoint provides Business Value to Lancaster University by:

1. Helps to identify privilege misuse, observe trends and investigate effectively
2. Enables 80-90% quicker response to cyberthreats
3. Saves 80-90% of time compared to "business as usual”

"Having central visibility and the ability to enrich logs in Logpoint is incredibly useful from a security perspective. Having identity-enriched logs means that we can spot privilege misuse, observe trends, investigate effectively and pick out issues pre-emptively before they become an actual problem"

John Couzins

IT Security Manager, University of Lancaster

Region Jämtland Härjedalen: Increases transparency by providing citizens quick and easy access to information

Region Jämtland Härjedalen is located in the middle of Sweden, bordering Norway to the west. With a population of around 127.000, it's one of the smallest among the 21 Swedish regions. But in terms of territory, it's the third largest.

Logpoint provides Business Value to Region Jämtland Härjedalen by:

1. Effectively monitors IT infrastructure and helps ensure compliance with the Swedish Patient Data Act
2. Increases transparency by providing citizens quick and easy access to information about the access and use of their medical records
3. Pinpoints unwanted and unintentional use of medical records, and helps improve user behavior via audit dashboards and log reports

“The Logpoint SIEM allows us to monitor the state of our infrastructure continuously and provides alerts if something out of the ordinary is occurring. In addition, it provides us with the necessary tools to drill down into an incident and to establish whether there is a technical problem, user error, or an actual breach of security"

Lars Christerson

Information Security Officer, Region Jämtland Härjedalen