Cybersecurity

# How to Write the Executive Summary of a Cybersecurity Report

Edward Kost

updated Oct 12, 2023

Let's face it, information technology experts are usually not enthusiastic writers. So when it comes to creating an executive report, cybersecurity staff aren't exactly pushing each other over to get this exciting writing task complete. Instead, it keeps getting delayed, day by day, until the night before its submission.

Many get stuck on the executive summary section, obsessing over its perfection. This is understandable since the executive summary is probably the most important component of the report. All stakeholders and decision-making staff judge the value of a report



If you're up late struggling to craft the perfect cyber security summary, use this template to finish your work quickly so you can finally get some sleep!

Contents



# Cybersecurity Executive Summary Example Template

The executive summary of your cybersecurity report is just that - a summary! Don't bloat it with technical explanations; that's what the body of the report is for (and even then, you should keep your technical ramblings restrained).

Your executive report should be tailored to the expectations of the leadership team, and most

stantly Generate
Cybersecurity
Executive Report
with UpGuard

of them don't want technical jargon.


The executive summary should succinctly summarize your security program efforts and address all of the high-level security concerns of the leadership team.

Learn about the main cybersecurity concerns of the executive team >

To tick all of these boxes, your executive summary should be comprised of the following headings:

- Key findings
- Security Risk Monitoring Summary
- Cyber Incident Summary
- Cyber Threat Summary
- Remediation Recommendations

This set of headings is characteristic of a classical method of structuring an executive summary for a security report.

While this classical structure is still acceptable, if you want to really impress the leadership team, consider using a more modern cybersecurity reporting style in your next reporting cycle (more details below).

# Key Findings

The key findings section is a high-level summary of the major cybersecurity threats encountered in the current reporting period. It should also summarize the

remediation efforts that addressed these risks and their efficacy.

Some examples of security incidents worthy of inclusion in this section are:

- **Phishing Attacks** - Especially the campaigns involving hackers posing as C-suite executives.
- **Critical Vulnerabilities** - Including zero-day exploits, such as Log4Shell and Spring4Shell.
- **Malware Injections** - Including failed ransomware attacks and other cyber attacks attempts.
- **Access Control Abuse** - Such as privilege escalation attempts.
- **Data Breaches -** The specific attack vectors that facilitated each security breach attempt.
- **Physical Security Threats** - Including lost hard-drives
- **Critical Service Provider Vulnerabilities** - Software misconfigurations and data leaks in the third-party ecosystem, whether linked to poor security practices or insufficient security controls.

Some threat mitigation details worthy of mentioning include:

- Incident Response Plan protocols that were activated for each listed cyber risk.
- Methodologies used to measure risk impact.
- The lifecycle of each security event.
- The impact on computer systems and information systems.
- Penetration tests that were performed to confirm security control efficacy.

- Security awareness training programs that were implemented to prevent repeated incidents.
- Firewall settings that were reconfigured to prevent similar network breaches in the future.
- Overall improvements to your cybersecurity program that were implemented to increase threat resilience.

The examples below purposely include more details than are required in an executive report summary. This is to help you understand the context of each cybersecurity aspect being addressed.

## Example of Key Findings and Mitigation Measures Summary

Here's an example of the key findings portion of a cybersecurity report executive summary and its subsequent mitigation measures.

### Example: Key Findings

1. ***Phishing Attacks:*** *There has been a notable increase in phishing attempts, particularly those imitating C-suite executives. These deceptive campaigns target our employees via email and SMS. Our incident response team detected and neutralized these threats, and we promptly provided additional training to our workforce to better identify such risks in the future.*
2. ***Critical Vulnerabilities:*** *We discovered and addressed several significant vulnerabilities during this quarter. Notably, the exposure to zero-day exploits such as Log4Shell and Spring4Shell*

*was promptly remediated with emergency patching and system updates, safeguarding our systems from potential breaches.*

3. ***Malware Injections:*** *There were a few failed ransomware attack attempts detected by our cybersecurity team. Our robust security defenses and proactive incident response successfully kept our systems secure and minimized potential damage.*

4. ***Access Control Abuse:*** *Our systems detected a number of privilege escalation attempts, indicative of potential internal threats. Subsequent investigations did not uncover any insider malfeasance. Still, we've strengthened our access control policies and added further surveillance mechanisms to preempt similar future attempts.*

5. ***Data Breaches:*** *We identified and thwarted several attempted breaches via different vectors, protecting our sensitive data from exposure. Enhanced security measures and updated policies are now in place to better guard against such attempts.*

6. ***Physical Security Threats:*** *A few instances of lost or misplaced hard drives were reported this quarter. In response, we tightened our physical security procedures and provided additional training to personnel on secure handling and storage of physical media.*

7. ***Critical Service Provider Vulnerabilities:*** *We discovered several software misconfigurations and data leaks within our third-party ecosystem. In collaboration with these providers, we've* rectified these issues and improved our oversight of third-party security controls.

## Example: Mitigation Measures

1. ***Incident Response:*** *The protocols outlined in our Incident Response Plan were activated for each listed cyber risk, ensuring a timely and effective response.*
2. ***Risk Impact Assessment:*** *We used various methodologies, including quantitative and qualitative approaches, to measure the potential impact of identified risks.*
3. ***Security Event Lifecycle Management:*** *Each security event was tracked from detection to remediation, ensuring complete visibility and control over our cybersecurity environment.*
4. ***Penetration Tests:*** *Regular penetration testing confirmed the effectiveness of our security controls and highlighted areas requiring further attention.*
5. ***Security Awareness Training:*** *A series of training sessions were conducted to increase employee awareness of cybersecurity threats and their role in maintaining our organization's security.*
6. ***Firewall Configurations:*** *We made significant adjustments to our firewall settings to improve our network's resilience to potential breaches.*
7. ***Cybersecurity Program Improvements:*** *Several improvements were implemented in our cybersecurity program, including new software solutions and process optimizations, to enhance our overall threat resilience.*

Learn the best practices to follow when creating a cybersecurity board report >

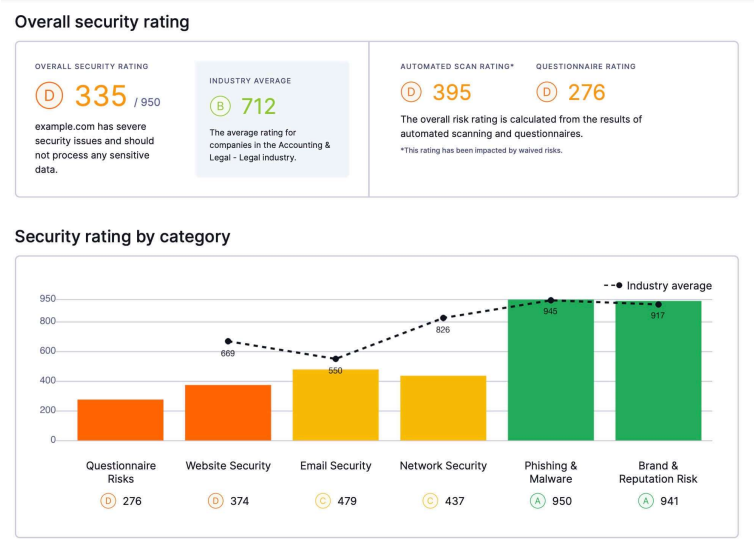
# Security Risk Monitoring Summary

Summarize the range of security risks and cyber threats monitored in the current reporting cycle. It's just as important to mention which regions of the IT ecosystem were not monitored and why.

Also, describe the risk monitoring methodology used, i.e., real-time attack surface monitoring.

Learn more about attack surface monitoring >

Security rating software is the most popular method of monitoring emerging security risks and security posture deviations. If your information security team uses such a tool, be sure to summarize the specific data security attack vectors influencing your security rating calculation.




Security rating distrubution across 6 attack vector categories - snapshot of UpGuard's vendor risk report.

Learn more about security ratings >

## Example of Security  Risk Monitoring Summary

*In the current reporting cycle, we continuously monitored a wide array of security risks and cyber threats across various components of our IT ecosystem. Our cybersecurity strategy was designed*

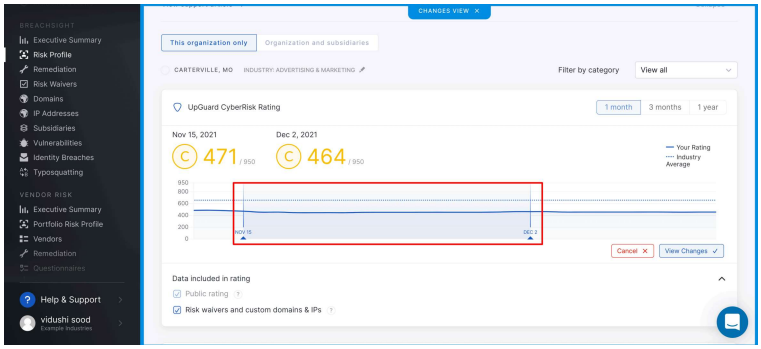
*to ensure comprehensive coverage while emphasizing areas more susceptible to threats.*

*Our real-time attack surface monitoring focused on the following key areas:*

1. ***Network Infrastructure:*** *Our team continuously monitored our routers, firewalls, and switches for any unusual activity. Vulnerabilities were promptly identified and patched to minimize the potential for exploitation.*
2. ***Applications and Services:*** *We employed regular scans and updates to detect and eliminate any vulnerabilities in our software applications and web services, reducing the potential attack surface.*
3. ***Endpoints:*** *Desktops, laptops, and mobile devices were monitored for signs of malware or other malicious activities. Our endpoint security solutions provided real-time threat detection and response capabilities.*
4. ***Cloud Assets:*** *Given our significant use of cloud-based solutions, continuous monitoring of our cloud environments was critical to promptly detect and mitigate any potential threats or vulnerabilities.*
5. ***Third-Party Attack Surface*** *- WIth data breaches caused by compromised third-party vendors on the rise globally, our attack surface monitoring solution is also continuously scanning our vendor network for vulnerabilities that could facilitate third-party breaches.*

*Our risk monitoring methodology included the use of security rating software, providing us with a valuable tool to identify emerging security risks and deviations from our security posture.*

*Our security rating drop during this reporting period was primarily influenced by a rise in phishing attempts and the discovery of critical vulnerabilities in some applications. Our team swiftly acted upon these insights, implementing robust countermeasures and reinforcing the security posture of our organization. The continuous monitoring and rapid response have allowed us to maintain a strong security rating and proactively manage our cybersecurity risk landscape.*




An example of security rating changes during a reporting period that would support this section of the report - A snapshot of the security rating tracking feature on the UpGuard platform.

- Learn how UpGuard streamlines Attack Surface Management >
- Learn how UpGuard calculates security ratings >

# Cyber Incident Summary

The security-related incident section is a more detailed delineation of the major remediation efforts mentioned under key findings. Focus on the most critical security incidents - those of the potentially greatest detriment to your security posture.

Such events in the third-party threat landscape are easier to track and identify if you're implementing a vendor tiering strategy.

Learn more about vendor tiering >

Demonstrate a commitment to continuous improvement by benchmarking your risk management efforts against security policies and key metrics such as Mean Time to Contain (MTTC), Mean Time to Resolve (MTTR), etc.

Read about the 14 cybersecurity KPIs you should be tracking >

Also, mention any specific security controls that prevented cyber incidents, such as multi-factor authentication or specific cybersecurity framework controls.

Learn more about the NIST Cybersecurity Framework >

Because this section of the report offers a deeper explanation of encountered cyber incidents, there's a risk of getting a little too technical with your wording. But don't obsess over keeping to a set baseline of simplicity. You have a technical representative on the executive team who can offer further clarification if required - the CISO.

## Example of a Cyber Incident Summary

*In this reporting period, we encountered several significant cybersecurity incidents. The main threats were:*

1. ***Phishing Attacks:*** *One of the most frequent incidents were phishing attempts impersonating C-suite executives. While the attacks were widespread, our multi-factor authentication controls prevented any unauthorized access.*

*Additional training was provided to all staff to improve awareness and prevention of future phishing attacks.*

2. ***Zero-Day Exploits:*** *The discovery of critical vulnerabilities, specifically the Log4Shell and Spring4Shell exploits, posed a significant risk. However, immediate remediation efforts and continuous monitoring enabled us to resolve these vulnerabilities before any harm could occur.*

3. ***Service Provider Vulnerabilities:*** *We identified potential threats from software misconfigurations and data leaks within our third-party ecosystem. With our vendor tiering strategy, we w*ere able to quickly identify and work with the affected vendors to resolve these issue.

*Throughout these incidents, the NIST Cybersecurity Framework guided our approach to managing cybersecurity risks. The framework helped us to identify potential threats, protect against them, detect incidents promptly, respond to them effectively, and recover efficiently.*

*These incidents were major tests of our security policies and protocols. To measure our effectiveness, we consistently monitored key metrics such as Mean Time to Contain (MTTC) and Mean Time to Resolve (MTTR). Our MTTC remained within acceptable levels, indicating our ability to quickly control incidents upon detection. Additionally, our MTTR showed a slight decrease, highlighting our commitment to resolving security risks as quickly as possible.*

# Cyber Threat Summary

The preceding section focused on the cyber incidents impacting your security posture, including those initiated by cybercriminals. This section should focus on emerging threats in your ecosystem, internally and throughout the third-party network.

Describe the mechanisms used to discover these threats, i.e., risk assessments.

Learn how to perform a cybersecurity risk assessment >

Cyber threats also include non-compliance with critical security regulations such as PCI DSS and HIPAA, especially for highly-regulated industries like healthcare.

## Example of a Cyber Threat Summary

*In the current state of our threat landscape, the following cyber threats have the highest potential of impacting our security posture. This list includes threats originating internally and within our third-party network.*

1. ***Advanced Persistent Threats (APTs):*** *We have identified some signs of APTs targeting our systems. Our risk assessments indicated a potential increase in sophisticated and targeted attacks that aim to gain unauthorized access to our sensitive information.*
2. ***Insider Threats:*** *While we have seen no specific incidents, our proactive risk assessments highlight the potential for threats originating internally. We are continually refining our access controls and monitoring systems to detect and prevent such risks.*
3. ***Third-Party Threats:*** *Our Vendor Risk Management process has identified potential threats emerging from our third-party network.*

*We are actively working with these partners to ensure they meet our security standards and reduce the associated risk.*

4. ***Non-Compliance Risks:*** *As a part of a highly-regulated industry, the threat of non-compliance with critical security regulations such as PCI DSS and HIPAA is always a risk. To mitigate this, we continuously update our compliance programs and train our employees on the importance of adhering to these regulations.*

*To discover these threats, we use a combination of mechanisms, including routine risk assessments, continuous monitoring, and proactive threat hunting. Our risk assessment methodology focuses on understanding the threat landscape, identifying vulnerabilities, assessing the potential impact and likelihood, and developing a risk treatment plan.*

- Learn how to communicate Attack Surface Management to the board.
- Learn how to communicate third-party risk to the board.

# Remediation Recommendations

This final section should summarize the necessary remediation processes for addressing the emerging risks mentioned in the preceding section. If these remediation initiatives require additional investment, include their approximate costs.

Justify the ROI of your investment requests by mapping them to the potential damage costs of the cyber risks

they will address.

Learn how to approximate the financial impact of cyber risks >

## Example of Remediation Recommendations

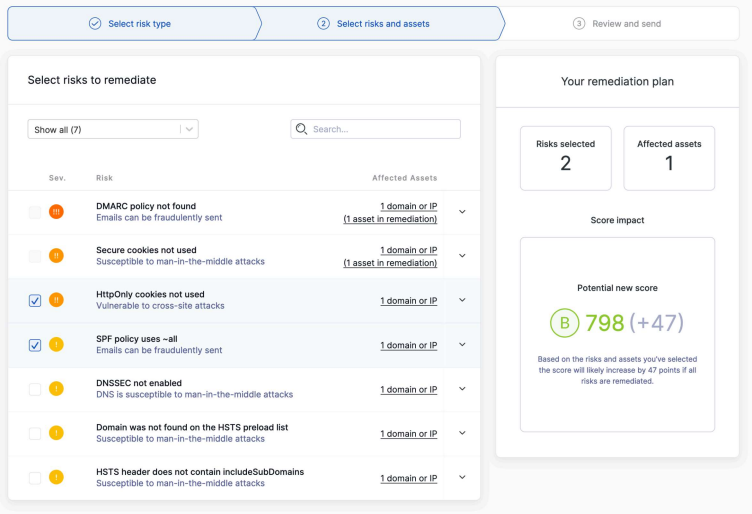
*The analysis of our security posture and emerging risks has led us to identify several necessary remediation initiatives. Here are our top recommendations for the next quarter, along with the estimated investment required for each:*

1. ***Enhanced Endpoint Security:*** *We recommend the deployment of an advanced endpoint detection and response (EDR) solution to improve threat detection and response capabilities. This requires an estimated investment of $25,000. Given the rise in phishing attempts and malware attacks, this investment can significantly reduce the risk of successful breaches, potentially saving hundreds of thousands in incident response costs.*
2. ***Third-Party Security Audit:*** *Given the potential threats arising from our third-party network, a comprehensive third-party security audit is recommended. This could cost around $15,000 but would ensure our vendors adhere to our security standards, thus reducing the risk of third-party data breaches.*
3. ***Compliance Training and Software Upgrade:*** *To mitigate the risk of non-compliance with PCI DSS and HIPAA regulations, we propose conducting additional compliance training for all staff and upgrading our compliance software. This is expected to cost around $10,000. The investment is justified considering non-compliance could lead to substantial fines and reputational damage.*
4. ***Insider Threat Monitoring Solution:*** *Implementing a solution for better detection and management*

*of potential insider threats is advisable. An investment of approximately $20,000 would support this initiative, significantly reducing the risk of internal data breaches which can lead to extensive damage costs.*

5. ***Advanced Persistent Threat (APT) Defense:*** *To combat the potential increase in APTs, we recommend an investment in a robust APT defense solution. This is expected to cost around $30,000, but the investment is vital given the severe damage that APTs can inflict on our organization.*

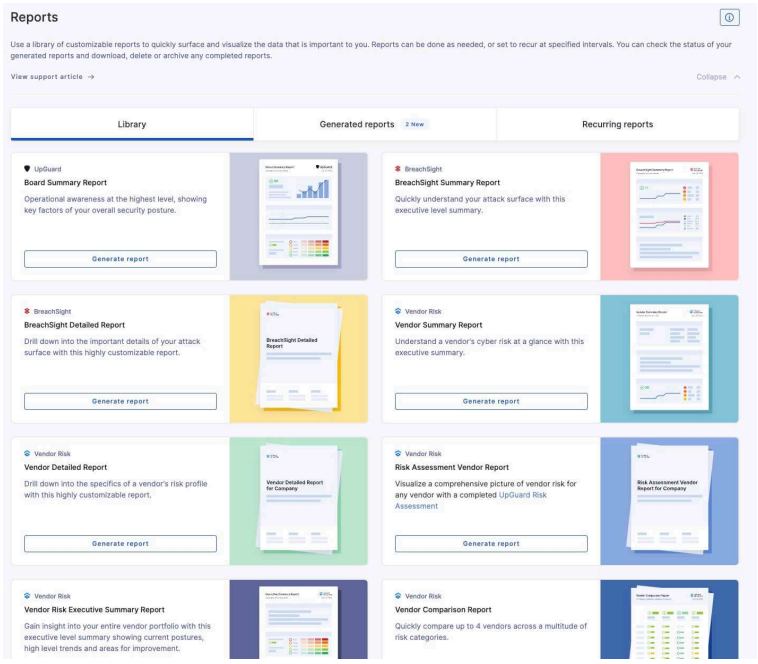
*In total, the recommended initiatives will require an estimated investment of $100,000. These recommendations are driven by a proactive approach to managing our cybersecurity risks. While this is a substantial investment, it is a necessary step in safeguarding our organization's sensitive data and systems from potentially devastating cyber threats. Considering the potential cost of damage from cyber threats, this investment is well-justified and will provide a strong return on investment by preventing costly breaches and non-compliance penalties.*




Including. a projection of the potential impact of remediation efforts on your security posture will help justify the value of suggested response actions - a snapshot of the security posture projection feature on the UpGuard platform.

# Instantly Generate a Cybersecurity Executive Report with UpGuard

UpGuard offers a range of customizable cybersecurity report templates to suit a range of stakeholder requirements in detailed and summarized editions.

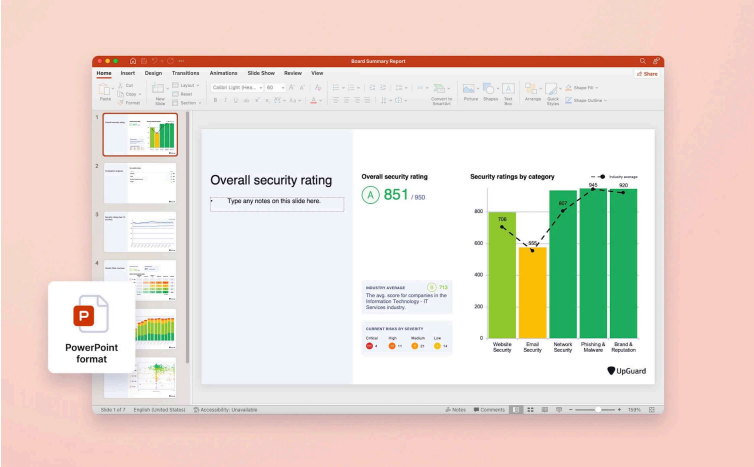



UpGuard's library of executive report templates

Graphical elements and charts represent the cybersecurity KPIs that matter most to executives, with charts and visual elements making your security efforts easier to understand and appreciate.

UpGuard's modern cybersecurity reports communicate your security efforts more efficiently than the classical executive summary structure outlined above. And they can be generated in just one click, so you don't need to stay up late writing them.

Once generated, a board summary report can be instantly exported as editable PowerPoint presentation slides, significantly reducing board meeting preparation time (and stress).




UpGuard's board summary reports can be exported as editable PowerPoint slides.

## Ready to see UpGuard in action?

Free trial

Tags: Cybersecurity

UpGuard

UpGuard is a complete third-party risk and attack surface management platform.

Contact sales | Free trial

**Products**

UpGuard Vendor Risk

UpGuard BreachSight

Security Ratings

Product Video

Pricing

Release notes

Integrations

**Compare**

BitSight

SecurityScorecard

CyberGRX

RiskRecon

All comparisons

**Tools**

Security Reports

Instant Security Score

**Solutions**

Financial Services

Technology

Healthcare

**Resources**

Breaches

Third-Party Risk Management

Attack Surface Management

Cybersecurity

**Company**

About us

Careers

Contact

Press

Support

Security

**Insights**

Events

Breaches

Resources

Blog

Glossary

News