infopulse • EBOOK

Enterprise Security in 2023-2024_

How to Define the Minimum Required Level of Security for Your Business?

AUTHOR

Kostiantyn Losinskyi

Expert Security Specialist with 15+ years of experience in the field

Table of Contents

Cybercrime today has become ubiquitous and more sophisticated than ever before. In 2023, approximately 560,000 new pieces of malware are detected every day, and each organization faces an average of **1248 cyberattacks per week**, as per Forbes. The imminent cyber risks that may cause significant financial losses, downtime, and reputational damage are urging businesses to strengthen their security posture. Yet, many companies have an insufficient level of security, as they still rely only on antiviruses, firewalls, and ad-hoc fixes, which is no longer enough to combat modern-day cyber threats.

In this eBook, we will overview the building blocks of cybersecurity systems and how they form five core enterprise security levels. Consequently, we will share the best practices on how to elevate your security level and achieve ultimate cyber resilience.

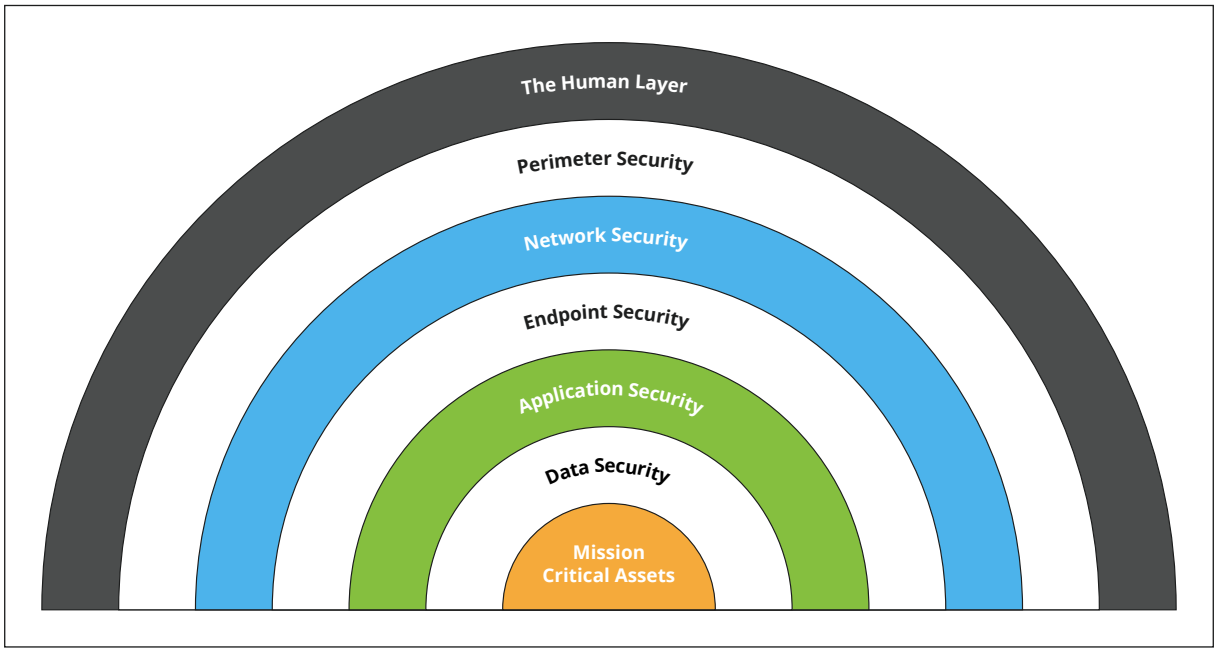
Key Pillars of a Cybersecurity System: Security Controls & Layers

Security controls are specific techniques, policies, and tools that are implemented to safeguard the organization's infrastructure and digital assets. Any countermeasure to reduce security risks can be considered a security control – from physical access cards to data loss prevention (DLP) tools or security awareness training sessions for employees. Security controls fall into three primary categories:

- **Physical** – fences, locks, surveillance cameras, access control, and intrusion detection systems
- **Administrative** – policies, guidelines, incident response processes, security education, and other activities related to personnel management
- **Technical** – controls aimed at protecting the organization's hardware and software, ranging from antiviruses and firewalls to SIEM/SOAR, threat intelligence, Security Operations Center (SOC), and other advanced security solutions.

To mitigate risks and reduce the impact of cyberattacks, security controls must be applied across different layers – the major facets of an organization that can be jeopardized by different forms of cyber risks. This approach is known as **"layered security"** or defense-in-depth. The idea behind this approach is that when a vulnerability is exploited at one layer, the security controls on the next layers will slow and hinder the threat until its eliminated.

Seven Core Layers of IT Security



Source

- **Human layer** – endangered by insider threats, human errors, and phishing attacks. Security controls to protect this layer typically include well-documented security policies and awareness training.
- **Perimeter layer** – ensures secure connectivity to the corporate network via routers and other devices. The perimeter is protected by firewalls, VPN, data encryption, and intrusion prevention tools.
- **Network layer** – often targeted by unauthorized access and DDoS attacks. To safeguard this layer, it's essential to implement managed LAN/WLAN, access control solutions, next-gen firewalls, and network monitoring tools.
- **Endpoint layer** – all corporate devices that are targeted by malware, ransomware, and zero-day attacks. This layer is best protected with endpoint detection & response (EDR) solutions.
- **Application layer** – covers the security of applications and their access to the organization's systems and data. To avoid broken authentication, injection attacks, and other threats this layer must be protected with continuous app patching, updates, access control (SSO/MFA), security monitoring, and penetration testing.
- **Data layer** – secures corporate data both in motion and at rest. The protection of this layer requires robust security controls across the application, endpoint, and network layers, as well as the implementation of data loss prevention tools, data classification, travel and sharing control, and data encryptions.
- **Mission-critical assets** – the final layer that is the primary target for the threat actors, as it stores the most valuable digital assets, such as user credentials, personal data, financial records, etc. In addition to counteractions from previous layers, mission-critical assets can be protected with coordinated incident response, data backup, and disaster recovery.

By analyzing what types of security controls are applied across each of the seven layers, you can identify the company's **level of security**, which is **the overall rate of your security maturity**. The formula for achieving a higher level of security is simple – the more advanced security controls you apply across each layer, the higher the security level you will gain. Although the risk scenarios and attack vectors depend on the organization's size, industry, services, and IT ecosystem, it's imperative to determine and establish the minimum required level of security to minimize risks and sustain cyber resilience.

What Are the Levels of Enterprise Security?

Our experts have outlined five core security levels that are based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework – a globally-recognized set of security standards and guidelines, as well as the Payment Card Industry Data Security Standard (PCI DSS) and cybersecurity policies and best practices from Microsoft. Each level is viewed from three perspectives – people, processes, and technology. Applying security controls across these three equally important domains is essential to safeguard any business from ever-evolving cyber threats.

Levels of Enterprise Security

Domains	People	Process	Technology
Entry Level	○ No dedicated security personnel or overlapping responsibilities ○ Outdated security qualifications or skills ○ Lack of security awareness	○ All security activities occur ad-hoc ○ Reactive approach to security management ○ No strategic or mid-term security management plans	○ No IT infrastructure standardization ○ Absence of centralized management ○ Lack of security visibility
Basic Level	○ Part-time or shared security personnel ○ Some vendor training sessions conducted ○ Basic security education for non-IT personnel	○ Clear communications flow between the IT and security teams ○ Security responsibility segregation is defined to a certain extent ○ Various security processes defined and documented ○ Security roles assigned across the organization	○ Certain security systems in place ○ Security solutions not fine-tuned ○ Several infrastructure components are managed centrally ○ Insufficient security visibility

Domains	People	Process	Technology
Challengers Level	○ Defined CISO functions ○ Ongoing security awareness training sessions ○ Security team is not fully staffed ○ Regular vendor training sessions conducted	○ Defined security strategy ○ Corporate assets labeled and categorized ○ Well-documented IT infrastructure ○ Security responsibility segregation is clearly defined ○ Measured and controlled security process metrics	○ Relevant security solutions in place ○ Centralized management of key security solutions and IT assets ○ Full security visibility over business-critical assets ○ Advanced security solutions used ○ Security solutions are updated to the latest versions and patches
Mature Level	○ Security teams are extended with third-party services ○ Defined common security roles ○ Highly skilled and educated security teams	○ High coverage of security processes ○ Regular security assessments ○ Process-driven IT and security management approach ○ KPIs for all major IT and security processes in place ○ Obtained security certifications ○ Secure-by-design approach	○ Security risk assessment solutions and technologies implemented ○ Security solutions regularly fine-tuned with respect to the changing cyber landscape ○ Regular validation of security controls ○ Automated upgrades to the latest versions and patches ○ Custom security solutions in use
Highly Secure Level	○ Red/Blue teaming with internal teams conducted ○ Bug-bounty program in place ○ Extensive security budget	○ Proactive approach to security management ○ Cooperation with third-party security teams or governmental bodies ○ Direct communications with vendors concerning the improvements of security solutions ○ RBAC and Least privilege approach implemented ○ Security best practices implemented and regularly reviewed	○ Enterprise-wide automation of security operations ○ Implementation of next-gen security solutions ○ Threat intelligence deployed ○ Complete security visibility ○ Multi-layered and multi-vendor security approach

How to Define the Minimum Required Level of Security?

Identify the Value of Your Mission-Critical Assets & Assess Risks

By evaluating the value of its data, an organization can accurately prioritize the required security controls. To illustrate the point – a small-scale e-commerce business is unlikely to be targeted by complex and costly zero-day threats, which means that aiming to reach the Highly Secure level is impractical. Yet, businesses that operate in highly-regulated industries and store large volumes of mission-critical assets and sensitive data, such as BFSI, healthcare, manufacturing, energy, and telecom, must obtain a Highly Secure, or at least a Mature security level.

After determining the value of your data, it's also important to assess the associated business risks by answering the following questions – What if your mission-critical assets are lost, leaked, and corrupted? How will data loss affect your business continuity? Is there a data backup and a disaster recovery plan?

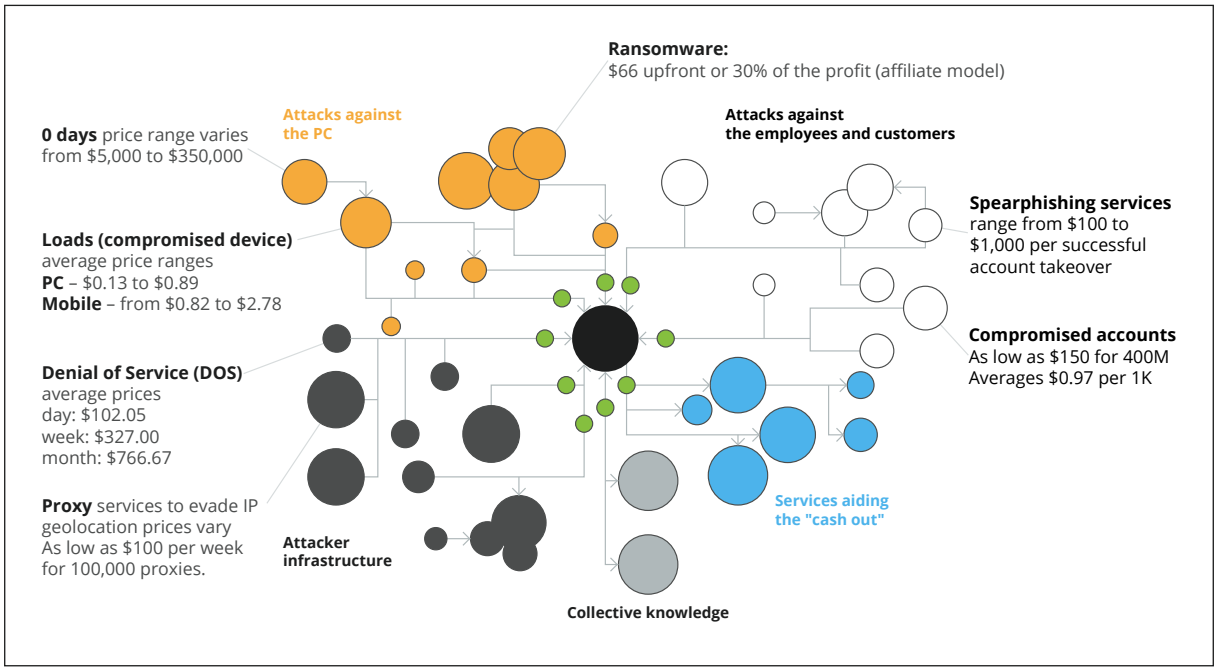
Once you have a clear picture of your assets and the related risks, it's easier to predict the possible attack vectors and strengthen the protection across the most vulnerable security layers.

Define the Data Value/Breach Cost Correlation

One of the major cybersecurity postulates states that the cost of hacking into your company must be higher than the value of assets threat actors can receive in case of a successful breach. For example, the value of your data is $5 million, but it requires $6 million to breach your security system – in such a case, it's pointless for cybercriminals to target your enterprise.

Unfortunately, this postulate is often ignored by companies that choose to cut down the security budget and neglect to apply security controls across multiple layers. This may have an adverse impact on one's business, as there is a definite breach price for each asset, user, and ultimately the entire company. Depending on the attack vector, the price may range anywhere from less than $1 and up to $350,000+ or even millions of dollars. The most sophisticated full-chain persistence zero-day, zero-click attacks that subtly inflict malicious code into mobile devices cost up to $2,5 million, according to Zerodium – a world-leading bug bounty platform.

Security Breach Price per Attack Vector



To maximize the breach costs for the attackers, you must accurately analyze the data value/breach cost correlation and invest in developing powerful security controls across all layers of your business. The best-case scenario is to build a system that can potentially be compromised only by complex zero-day threats, as they are the most expensive to execute.

Conduct a Security Assessment

The most reliable and efficient approach to defining both the current and minimum required security level is to conduct a security assessment that is intended to evaluate whether all administrative and technical security controls work correctly. By performing an end-to-end security assessment, you can gain a 360-degree view of your security posture, discover hidden vulnerabilities across your IT architecture, and identify missing security policies and processes. The insights gathered during the assessment can serve as the foundation for a security level enhancement roadmap.

CASE IN POINT

How Security Audit Helped Bosch Reduce Business Risks

Learn more

Bonus: Example of a Security Level Enhancement Roadmap

Organizations can design and implement dedicated roadmaps to elevate their security level. The best option is to build a tailored roadmap that is based on a specific business case (industry, data value, business needs, etc.), as well as the security assessment insights and custom threat modeling results. This is an optimal approach, as the required security level depends on the company's size, services/products, business processes, and budget constraints, which makes reaching an entirely Highly Secure level across all segments rather challenging, or even unnecessary. The key goal is to move away from the Basic/Entry levels and build a blend of Challengers/Mature/Highly Secure levels that resonates with the company's needs.

The table below demonstrates an example roadmap that Infopulse developed for a large-scale European manufacturer with presence in over 30 countries and 3,500+ employees. The boxes colored in yellow indicate the client's initial security level across different segments, and the green ones show the levels that we aimed to achieve.

Eventually, Infopulse helped the client switch **from a primarily "Entry" level to a combination of Mature and Highly Secure levels** and strengthen its security posture with a 24/7 SOC enhanced with a cloud-based SIEM/SOAR.

Security Level Enhancement Roadmap

Segments	Enterprise Security Levels				
	Basic	Entry	Challengers	Mature	Highly Secure
Infrastructure Protection		✓		✓	
Security Visibility		✓		✓	
Endpoint Protection			✓		✓
External Perimeter Security		✓		✓	
Ransomware Protection		✓			✓
Identity & Access Security			✓		✓
Phishing Protection		✓			✓

Segments	Enterprise Security Levels				
	Basic	Entry	Challengers	Mature	Highly Secure
Zero-day Protection	✓			✓	
DDoS Protection	✓		✓		
Network Security		✓		✓	
Security Awareness of Employees		✓		✓	

*ORANGE – Initial security level *BLUE – Goal security level

What's Next?

The growing volume and complexity of cyberattacks pose a significant risk for both SMBs and large enterprises, especially those that possess large volumes of mission-critical assets. If your security system is poorly protected, threat actors can detect and exploit vulnerabilities often with little to no effort and expense.

By elevating your security level to a blend of Challengers/Mature you can keep the attackers at bay and avoid disastrous business risks. Moreover, by achieving a mostly or entirely Highly Secure level, you can transform your security system into a multi-layered cyber stronghold, capable of withstanding the never-ending swarm of cyberattacks, including even the most complex zero-day threats.

See how Infopulse helped Bosch and ING Bank level up their protection.

infopulse

CASE STUDY #1

Case for **Bosch**

Infopulse Conducts Security Audit of Embedded Solutions for Bosch_

Bosch reduces business risks and improves software quality of the products

Industry: **Manufacturing** **Location:** **Germany** **Employees:** **10,000+**

Website: **www.boschsecurity.com**

Customer: **Bosch** Industry: **Manufacturing** Location: **Germany** Employees: **10,000+**

Business challenge

- Bosch Security and Safety Systems has been the customer of Infopulse since 2007, with many successful projects implemented together.
- This time, Bosch asked us to conduct an independent security audit to ensure the security of different client-server and embedded solutions.

Solution

- Full specifications of the technical security assessments approved with the customer.
- The whole scope of security services, namely penetration tests and deep technical security analysis of the physical security management solutions and the devices' embedded software: application binaries, configurations, data, traffic, protocols, interfaces, encryption, databases, etc.

Business value

Bosch received comprehensive reports on security risks and vulnerabilities with strategical and tactical recommendations on mitigating threats and improving security, including the following benefits:

- Reduced security costs;
- Lowered business risks;
- Improved quality of the software products to be delivered to the end-customers worldwide.

Types of services

- Security assessment
- Threat and risk analysis
- Penetration testing

Standards & Tools

NIST SP800-115 | PTES | OWASP | EC-Council

ISF SoGP | BSI IT-Grundschutz

Customer Quote

The Bosch brand is a global leader in quality and innovations. Our product philosophy is to build reliable and trustworthy solutions with adherence to the highest industry standards. By making valuable contributions to the development of our products, Infopulse has proven to be a productive, efficient, and reliable partner for Bosch Security & Safety Systems. We would like to express sincere appreciation for the quality of services delivered by the Infopulse security team.

Harald Schoengen

Senior Manager at Bosch Security & Safety Systems

infopulse

CASE STUDY #2

Case for **ING Bank Ukraine**

Penetration Testing Against Information Security Risks for ING Bank_

Industry: Banking & Finance **Location:** Ukraine **Employees:** 63,000+ (global)

Customer: **ING Bank Ukraine**

Industry: **Banking & Finance**

Location: **Ukraine**

Employees: **63,000+ (global)**

Client background

Headquartered in Amsterdam, Netherlands, The ING Group is a global financial corporation with 150-year background. ING Bank's more than 63,000 employees offer retail and commercial banking services to over 32 million private, corporate and institutional clients in over 40 countries. ING Wholesale Banking Ukraine is a full subsidiary of ING, a leading global financial institution with a strong European base.

Business challenge

Aiming to enhance the protection of the Internet services against web-hacking attacks, the bank intended to identify all security weaknesses of the web applications and mitigate the risk of misusing the network services.

Solution

Vulnerability Assessment

Discovering all vulnerabilities in the target web and application servers with the use of known automated tools, e.g. Web Inspect, and the developed specific tests.

Penetration Testing

Attack the target systems with the aim of confirming the identified vulnerabilities and discovering the other undetected ones.

Security Test Reporting

Report all identified vulnerabilities, implications and countermeasures.

Business value

The security testing approach was essentially based on OWASP security testing guidelines.

Based on the obtained security test report, ING Bank has improved the protection measures for the business-critical web applications.

Types of services

- Security assessment
- Threat and risk analysis
- Penetration testing

Standards & Tools

OSSTMM | OWASP | Offensive Security | SANS

ISSAF | ISACA

About Infopulse

Infopulse, part of the leading Nordic digital services company Tietoevry, is an international vendor of services in the areas of Software R&D, Application Management, Cloud & IT Operations, and Cybersecurity to SMEs and Fortune 100 companies across the globe. Founded in 1991, the company has a team of over 2,000 professionals and is represented in 7 countries across Europe and the Americas.

Infopulse is a Global Outsourcing 100® company recognized by IAOP® and trusted by many established brands, such as Allianz Bank, BICS, BOSCH, Corteva Agriscience, Credit Agricole, Delta Wilmar, ING Bank, IPCO, Metinvest, Microsoft, Offshore Norge, OLX, OTP Bank, Raiffeisen Bank Aval, Santander, UkrSibbank BNP Paribas Group, Vodafone, Zeppelin, and others.

For more information, please visit **www.infopulse.com**

About the Author

Kostiantyn Losinskyi is a security specialist with 15+ years of experience in the field. His expertise focuses on systems and network security, pentesting, auditing, security solutions architecture, and SOCs. Kostiantyn's competence is supported by numerous certifications from the industry's top vendors, including IBM, Check Point, Cisco, and more.

Kostiantyn Losinskyi

Expert Security Specialist with 15+ years of experience in the field

Not sure where to start with your security upgrade? Talk to Infopulse security experts to define your security maturity and next steps.

Let us help

info@infopulse.com