# Building resilient business solutions: Creating cyber-secure products to safeguard against vulnerabilities


Ignitec

**We are an award winning product design consultancy,** we design connected products and instruments for pioneering technology companies.

# Building resilient business solutions: Creating cyber-secure products to safeguard against vulnerabilities

Reading time 9 mins

## Key Points

- The cyber-threat landscape is evolving at an alarming rate, with the cost of cybercrime predicted to hit $8 trillion in 2023 and grow to $10.5 trillion by 2025.
- In an environment where time-to-market is often seen as a key to success, it makes more economic sense for many businesses to fix security problems if/when they arise after product launch.
- However, this ‘bolted-on’ approach is costly when faced with a cyber attack: products often must be redesigned, customers compensated, and business reputations repaired.
- Security by Design is a ‘baked-in’ approach to product development that prioritises integrating security measures into product design from the outset.
- Key elements of cyber-secure products include end-to-end encryption and multi-factor authentication, secure configuration and default settings, and user-friendly security features.
- Collaborating with consultancy firms that are Cyber Essentials Verified ensures that vulnerabilities are addressed, users are protected, and businesses are resilient against future threats.

**Looking for robust cyber-secure product development solutions? Call us for a quote!**

Get in touch

## Ben Mazur

Managing Director

Last updated Dec 12, 2023

**I hope you enjoy reading this post.**
If you would like us to develop your next product for you, click here

Share
Share
Tweet
Pin

As the reliance on technology grows, the need for products fortified with robust cybersecurity features that protect users' privacy and data has become increasingly imperative and a paramount concern for businesses. Most companies across industries seek innovative and comprehensive design solutions for cyber-secure products that protect their assets and maintain trust among their customers. Still, for some, these solutions aren't a priority.

In an environment where time-to-market is seen as the key to success, cybersecurity often takes a backseat to other efforts (e.g. prototyping) that advance the functionality of a new product. For some businesses, especially those on a budget, it makes more economic sense to fix security problems if or when they arise after the product's launch. The downside with this approach is that if the worst-case scenario does happen, products often need to be redesigned, customers compensated, and tarnished company reputations restored.

While the investment in cyber-secure product design might seem costly, it beats the alternative of resolving security breaches further down the line. Ignitec® is Cyber Essentials Certified, meaning that security is 'baked into' our product development process from the beginning rather than 'bolted on' at the end. Call us for a quote or a free consultation with one of the experts on our team to discuss

cyber-secure product development solutions. We'll help you address vulnerabilities and keep your business and customers safe – without breaking the bank!

### Related services

### Comprehensive Product Design Consultancy Services

### Cyber Essentials Verified

### Product Manufacturing Services

# What are the stakes, and why is 'security by design' important?

Cyber threats are evolving at an unprecedented pace. From sophisticated phishing attacks to ransomware and data breaches, the risks are multifaceted and ever-present. With recent high-profile attacks targeting healthcare, finance, retail, government, manufacturing, and energy, it's clear that the cyber-threat landscape is evolving at an alarming rate. According to Cybersecurity Ventures, the cost of cybercrime is predicted to hit $8 trillion in 2023 and will grow to $10.5 trillion by 2025.

Consequently, developing cyber-secure products with built-in security measures is no longer an option. Instead, it's a fundamental requirement for businesses seeking to protect data, maintain integrity, and fortify resilience against potential breaches.

"Security by Design" is an approach to software, hardware, and product development that prioritises integrating security measures and protocols throughout the design, production, and manufacturing process. Customer security is hence seen as a core business requirement and not just a technical feature, and is a proactive strategy that's 'baked in' instead of 'bolted on'.

Ensuring that security is an integral part of the overall structure and functionality involves anticipating potential security threats, risks, and vulnerabilities and addressing them early in the development lifecycle. Key elements include:

1. **Risk Assessment:** Identifying potential threats and vulnerabilities a system or product might face.

2. **Implementing Controls:** Integrating security controls, such as encryption, access controls, and authentication methods, at every stage of development.
3. **Compliance and Standards:** Ensuring adherence to relevant industry standards, best practices, and legal compliance.
4. **Ongoing Review and Improvement:** Continuously monitoring, testing, and updating security features to adapt to new threats and vulnerabilities.

By adopting this approach, we can minimise the risk of security breaches, data leaks, and cyber attacks. In addition, security by design promotes a proactive security culture that fosters trust and confidence among users and customers by demonstrating our commitment to protecting their data and privacy.

# 13 best practice essentials for cyber-secure product design

Product design is more than just how a product looks; it's about how it works from both user experience and technical perspectives. Critical components for best practice product design for cybersecurity include:

## 1. End-to-End Encryption

Ensure that data remains encrypted during transmission, storage, and processing. This prevents unauthorised access to sensitive information, even if intercepted.

## 2. Multi-Factor Authentication

Adding an extra layer of protection by requiring multiple forms of verification. Strong authentication and access control ensure that only authorised users can access sensitive information or features within the product.

## 3. Continuous Monitoring and Patching

Continuously monitor the product for vulnerabilities and promptly apply security patches and updates to address any discovered weaknesses.

## 4. User-Friendly Security Features

Balancing robust protection with a seamless user experience. Talk to your users or customers regularly to determine how and why they use your product. For example, if your product has software built into it, do users install security updates that are recommended? If not, why not?

## 5. Inclusive Design and Accessibility

Almost one in four people in the UK have some form of disability. Cyber-secure products should also be designed inclusively, with accessibility and protection for vulnerable users such as people with disabilities, elderly people, and people who are colourblind at the forefront.

## 6. Risk Assessment and Threat Modeling

Identify potential risks, vulnerabilities, and threats that the product might encounter. Understanding these risks allows for the implementation of targeted security measures. Download our free risk assessment template to get started and help keep your bases covered.

## 7. Secure Software Development Practices

Adhere to secure coding standards and best practices during the development process. This will reduce the likelihood of introducing vulnerabilities into the product's codebase.

## 8. Privacy Protection

Incorporate features that respect user privacy by limiting the collection and use of personal data. Ensure compliance with relevant privacy regulations and laws.

## 9. Secure Configuration and Default Settings

Set secure default configurations for the product to minimise the chances of exploitation due to default vulnerabilities.

## 10. Thorough Testing and Validation

Conduct comprehensive security testing, including penetration testing and vulnerability assessments, to identify and remediate any weaknesses or loopholes.

## 12. User Education and Training

Provide educational materials and training for users to promote awareness of cybersecurity best practices and how to use the product securely.

## 13. Incident Response and Recovery Plan

Have a well-defined incident response plan to effectively respond to security incidents or breaches, minimising their impact and facilitating recovery.

By incorporating these elements into the product design and development process, companies can create products that prioritise cybersecurity, reduce the risk of cyber threats, instil trust and confidence, and emphasise their reliability.

# A final word on designing cyber-secure products

Creating cyber-secure products with top-notch security requires a multi-layered strategy. It's about integrating security measures from the very outset of the product development lifecycle and implementing a proactive risk mitigation strategy. It's also about collaborating with cybersecurity experts or product design consultancy firms to ensure that products are fortified against potential vulnerabilities and comply with industry standards and regulations.

At Ignitec®, we treat our client's data – and our own! – with extreme care and take our commitment to privacy and security seriously. We understand that there isn't a one-size-fits-all cybersecurity solution; therefore, we ensure that the products we design are built to address your current and future needs – without breaking the bank. Call us for a chat, quote, or free consultation.

If you found this post helpful, please share it!



## A product risk assessment template to help you identify safety hazards

## Consumer consent, privacy and ethics of wearables

## Designing Assistive Technology: Empowering Smartbox Users Through Innovation

# FAQ’s

### Why are cyber-secure products essential for businesses?

Cyber-secure products are essential for businesses to safeguard sensitive data, maintain customer trust, and mitigate the risks of cyber threats and potential breaches that could result in reputational damage and financial loss.

### How can businesses ensure their products are cyber-secure?

Businesses can ensure their products are cyber-secure by implementing robust security measures like encryption, access controls, regular risk assessments, and following the principles of Security by Design throughout the development process.

### What characteristics define a cyber-secure product?

Cyber secure products feature strong authentication measures, end-to-end encryption, regular security updates, secure software development practices, and a well-defined incident response plan.

### When should businesses start implementing cyber security measures in product development?

Businesses should start implementing cyber security measures from the initial stages of product development, ensuring security is integrated into the product architecture from the outset.

## Which industries benefit most from having cyber-secure products?

Industries such as finance, healthcare, technology, and e-commerce benefit significantly from having cyber-secure products due to the high sensitivity of data and the potential consequences of security breaches.

## How do robust access controls contribute to cyber-secure products?

Robust access controls significantly contribute to cyber-secure products by limiting access to sensitive information and preventing unauthorised entry.

## What role does encryption play in ensuring cyber-secure products?

Encryption plays a vital role in ensuring cyber-secure products by safeguarding data from unauthorised access or interception, ensuring its confidentiality and integrity.

## Why is user education an essential part of ensuring cyber-secure products?

User education is essential in ensuring cyber-secure products as it empowers users to understand and apply cybersecurity best practices, reducing the risk of vulnerabilities due to human error.

## How can businesses create a culture of cybersecurity to support cyber-secure products?

Businesses can create a culture of cybersecurity by promoting awareness, providing regular training, and encouraging proactive security measures among employees, fostering a security-conscious environment.

## What are the best practices for testing the security of cyber-secure products?

Best practices for testing the security of cyber-secure products include conducting penetration testing, vulnerability assessments, and continuous monitoring to identify and remediate security weaknesses.

## Why is incident response planning crucial in cyber-secure product development?

Incident response planning is crucial in cyber-secure product development as it helps businesses respond effectively to security incidents, minimising their impact and facilitating a quicker recovery.

## How do regulations and standards influence the development of cyber-secure products?

Regulations and standards play a significant role in influencing the development of cyber-secure products, providing guidelines and benchmarks that businesses must adhere to to ensure security and compliance.

## What impact does the development of cyber-secure products have on customer trust?

Developing cyber-secure products enhances customer trust by assuring users that their data is secure, leading to increased confidence in the product and the brand.

## Why is it essential for businesses to stay updated with cybersecurity advancements for product development?

Staying updated with cybersecurity advancements is crucial for businesses to adapt to evolving threats, implement the latest security measures, and remain proactive in protecting their products against emerging risks.

## How can small businesses implement cyber-secure product strategies on a limited budget?

Small businesses can implement cyber-secure product strategies on a limited budget by prioritising essential security measures, leveraging open-source tools, and utilising free resources for training and education.

## What are the common challenges in implementing cyber-secure product designs?

Common challenges in implementing cyber-secure product designs include balancing security with usability, resource constraints, and the evolving nature of cyber threats that necessitate constant adaptation.

## When should businesses conduct security audits for their cyber-secure products?

Businesses should conduct security audits regularly for their cyber-secure products, preferably as part of a routine, to identify vulnerabilities and ensure ongoing protection against potential threats.

## What are the advantages of investing in cyber-secure product development consultancy?

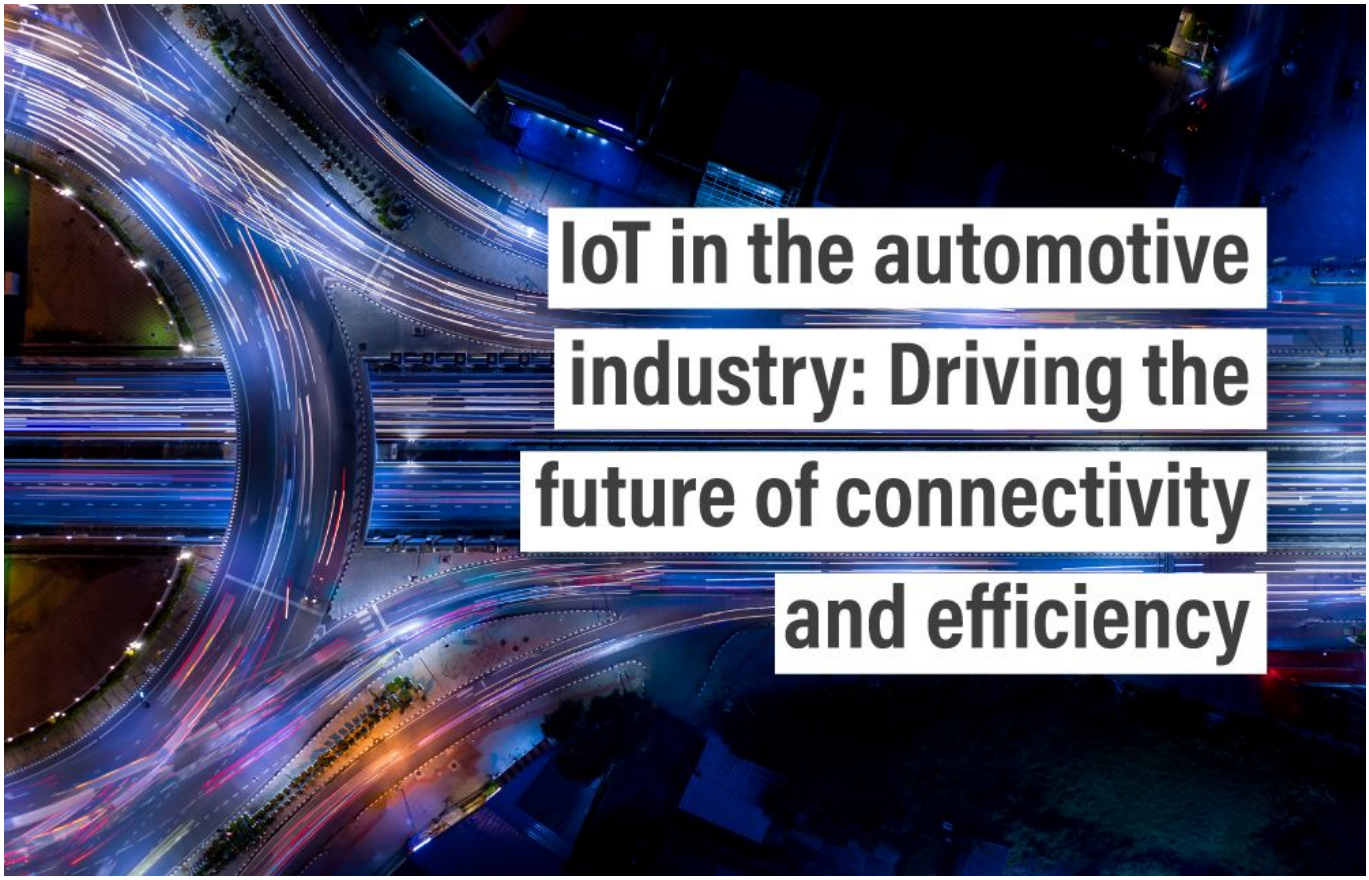
Investing in cyber-secure product development consultancy offers businesses expert insights, guidance on best practices, and tailored strategies to create robust security measures aligned with industry standards.

## How does the development of cyber-secure products impact the overall cybersecurity landscape?

Developing cyber-secure products positively impacts the overall cybersecurity landscape by setting industry standards, driving innovation in security technologies, and promoting a culture of proactive risk mitigation.

Share
Share
Tweet
Pin

Up next




## IoT in the automotive industry: Driving the future of connectivity and efficiency

Last updated Jun 27, 2024 | INNOVATION, INSIGHTS, PRODUCT DESIGN, SUSTAINABILITY, TRANSPORTATION

Discover how IoT in the automotive industry enhances vehicle connectivity, safety, and efficiency with cutting-edge technology.

read more