OneShield®
Cybersecurity Series

Cybersecurity & Innovation

Cybersecurity & Innovation

Core System Security

Ongoing demand in the insurance industry for digital engagement, improved customer experiences, and expanding digital ecosystems has broadened the role of and demands upon core technology systems. With the rise of SaaS solutions propelling insurers to adopt emerging technologies at a faster pace then ever before - ensuring security requirements can keep pace with technology adoption is imperative.

Protecting the Core of Your Technology Platform

Emerging Risks

- As insurers transition from internal development of technology to integrating with innovative third-party solutions, the vulnerabilities of each partner become a potential threat to the insurer's environment. Expanding your technology ecosystem requires domain expertise to assess vendors and the security of each touchpoint.
- Increased use of APIs requires rigorous testing and adherence to industry security standards.
- Increased mobility needs of hybrid and remote workers require secure device management.
- Cybercriminals are becoming increasingly sophisticated in their methods, and their innovation is well funded. Quantum computing will eventually crack encryption, and insurers must prepare to adopt post-quantum cryptographic standards.
- Security breaches and ransomware are increasing at an alarming rate.

Creating a "security-first" culture in your company is critical to managing current and future risks. The more your organization understands about cybersecurity, compliance obligations, best practices, vendor assessments and the tools available, the more equipped your organization is to move forward in securing business transformation.

Key Recommendations

- Align your security program with business goals for executive buy-in and investment.
- Embrace and champion a culture of awareness and strict adherence to security best practices by implementing a security program and framework which improves your products and corporate security posture.
- Understand the regulatory environment that applies to the security and privacy aspects of your business operations and identify the crucial controls required to ensure adherence to compliance and consumer confidence in your products.
- Choose a technology vendor and partner that has security uppermost in the design and implementation of your business's digital platform to make certain your core system environment is secure.

Core System Security

We've identified some of the emerging risks associated with rapid innovation. Within this guide we offer 14 key disciplines and protocols to reach your potential while securing your innovations.

But first, let's review the reasons these practices are so important.

The Future of Cybersecurity

"It's going to be disruptive over the next couple of years as we prepare for the impact of quantum computing, as cryptology standards will need to change based on the emerging threat. The industry is going to have to decommission older technology and making sure that we're not still accepting pre-quantum cryptographic solutions and we're going to have to alert IT departments of the new standards. It will be a lot of work preparing and deploying the new standard.

Having a partner like OneShield who understands the need for security is critical. OneShield has tremendous backing and investment - with an investment source and executive team that understand the importance of cybersecurity and more importantly, the prioritization of it. Secure insurance products are our business and we've been doing it for over two decades."

- Chad Galgay, CISO, OneShield

Excerpt from PropertyCasualty360° series Top Tech Trends from Insurance Leaders, Chad Galgay, Chief Information Security Officer at OneShield, discusses cyber risk trends and their impact on insurers' tech ecosystems. Listen here

Secure Your Future

Increased personalization, the flexibility of offerings, real-time pricing changes, consumer-activated insurance, and other product innovations can be the difference in responding to ordinary and extraordinary market disruptions. The more you are aware of cybersecurity and the tools available, the more equipped you will be to move forward in securing your future transformation.

OneShield has always placed security best practices at the forefront of every aspect of our company culture and software development processes. This is critical to protecting our clients' interests, and to providing solutions that improve the experience between people and insurance products. We provide built-in security that meets industry best practices and the regulatory compliance needs of our clients.

A successful cybersecurity approach has multiple layers of protection spread across the whole of an operation. The people, processes, corporate culture, and technology approach must all complement one another to create an effective defense from cyber-attacks.

Cybersecurity Defined

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

It's also known as information technology security or electronic information security. These malicious attacks (cyber-attacks) are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes.

Implementing effective cybersecurity measures is particularly challenging today amid economic disruption, an explosion of devices outnumbering people, and rapid innovation of criminal tactics.

There are many new and evolving security tools and best practices to better understand the breadth of security controls available to help protect your organization's data. It's important to increase your security posture; and secure your apps, data, and network across cloud and hybrid environments.

Cyber Security Studies Reveal a Costly Landscape

Worldwide spending on cybersecurity is forecast to reach

$347 billion in 2023

(CybersecurityVentures)

From 2016 to 2021, web application breaches against the financial/insurance sector

increased from 12% to 51%

(Verizon)

Cyber risk ranks #1 in 2022

as most important business risk by global risk manager / business leaders

(Allianz Risk Barometer) / (Travelers Risk Index)

More than 1 in 5 firms attacked say solvency was threatened

An increase of 24% from the prior year

(Hiscox Cyber Readiness Report 2022)

The average cost of a data breach for critical infrastructure organizations studied was

$ 4.82 million in 2022

($1 million more than the average cost for organizations in other industries)

(IBM)

Every 11 seconds, an organization suffered a ransomware attack in 2021

Expect an attack every 2 seconds by 2031

(CybersecurityVentures)

Compliance is a Moving Target

To date, there are no laws dictating how to protect your business. But incrementally, legislation is being introduced to handle data breaches.

It is critical that as unified legislation around data protection is achieved - insurers need to ready their operations to be able to expand the definition of personal information and prepare for mandates and implementation of information security requirements by proactively establishing guiderails for collecting, safeguarding, reporting and tracking of customer data.

In 2021, the Uniform Law Commission approved the Uniform Personal Data Protection Act (UPDPA) to support consistent state legislation. In 2022, Nebraska, Oklahoma, and the District of Columbia introduced but did not pass the UPDPA legislation, while other states continued to independently draft legislation.

The following are important privacy protection laws to understand and monitor as they continue to evolve, influence other legislation, and impact data management obligations:

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)*
- Colorado Privacy Act (CPA)*
- Virginia Consumer Data Protection Act (VCDPA)*
- Australia NDB Scheme
- New York Department of Financial Services cybersecurity regulation 23 NYCRR 500

*Take effect in 2023

Understanding the implications of and adhering to the multitude of standards is challenging. The General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) introduced many consumer privacy implications.

How you collect, store, report on, and delete consumer data is critically important. Consumer data rights continue to be at the forefront for lawmakers and their constituents.

These rights translate into business requirements, that your systems must be prepared to handle. A flexible and configurable core system is critical to easily retool and respond as requirements evolve.

"Ransomware is one of the biggest challenges the industry has faced in the last two years. To adequately mitigate this risk, make sure that you've got a good security program. Be on top of patching your system and ensure you've got a good endpoint detection response solution in place. And by all means, seek out industry experts and partner solutions to strengthen your security profile where you find internal deficits."

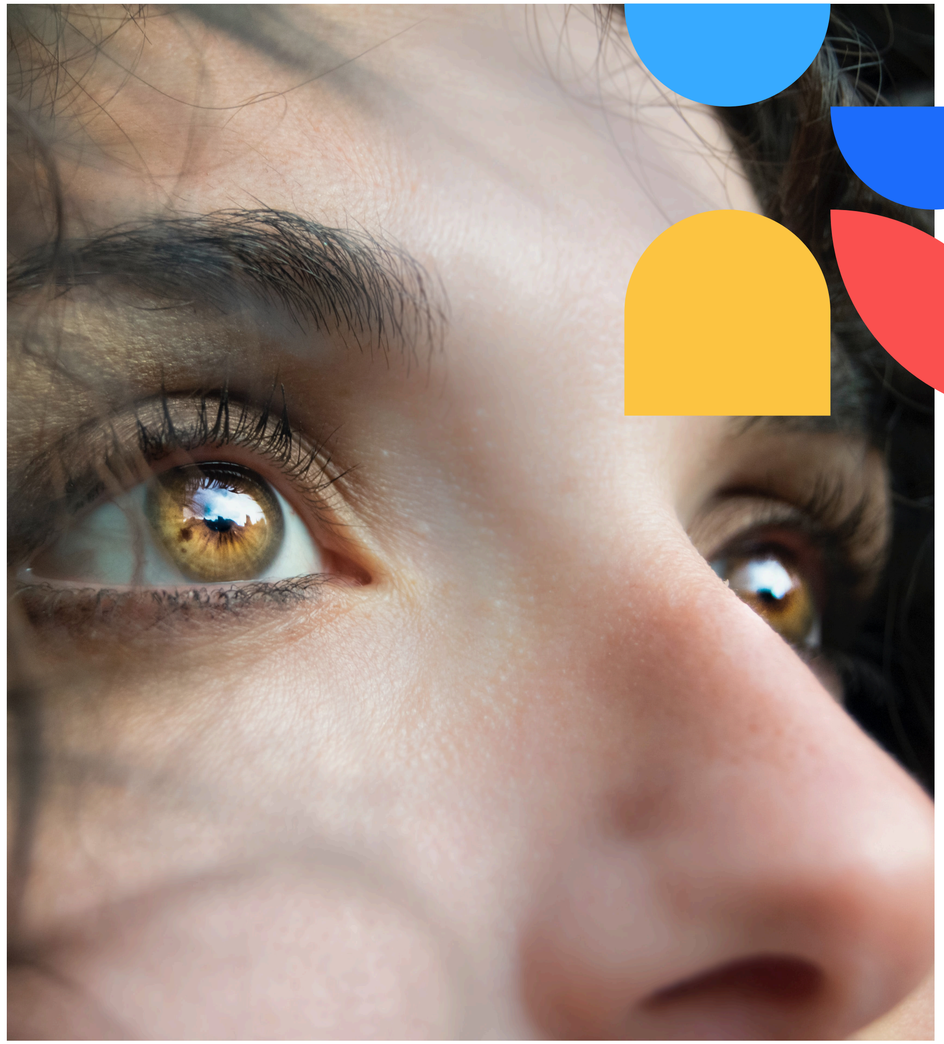
- Chad Galgay, CISO, OneShield

Embrace and champion a culture of strict adherence to security best practices through awareness and training.

Understand this is never a one-and-done task. Security practices must adjust as the possible risks to the environment change, and continual training is imperative to address these changes.

In addition, incorporate industry and compliance standards into every IT project and make sure all workflows, processes and business objectives align with security objectives.

To support your initiatives, we offer you 14 disciplines, practices, and protocols to remain secure, alert, and prepared in this rapidly evolving environment.



What Keeps You Secure?

Keeping your organization's operations secure requires a series of disciplines, protocols, and practices. Consider these security measures for your organization:

1 Development Program

Adopt a software development program based on proven industry secure frameworks and controls with security checks throughout the software development lifecycle.

2 API

A significant number of cyber-attacks target the business logic and APIs. Most often, security testing is limited to penetration tests, Static Application Security Testing (SAST), and Dynamic Application Security Testing (DAST), which does not address the growing concerns with API breaches and RBAC (Role-Based Access Control). Given this vulnerability, OneShield uses automation to test the security of its API and microservice architecture throughout the software development lifecycle.

3 Authentication

Authentication services are key to controlling who has access to your systems. For example, our clients can use OneShield's native authentication or integrate another preferred Identity Provider (IDP). OneShield supports many Multifactor Authentication (MFA) options and a range of modern security factors for implementation flexibility.

4 Web Service

Encrypting Web Services to ensure authentications, encoding and data integrity is imperative. At OneShield, all our web service integrations are built using transport confidentiality, server authentication, user authentication, transport encoding, and message integrity. Web services are encrypted using TLS with certificates from trusted providers and digital certificates for files and documents.

5 Single-Sign-On (SSO)

Integrate your software applications with a single sign-on portal through SAML 2.0 integration for secure identity management.

6 Object-Level Authorization

Establish specific role-based authorization and access for users and groups. For example, authorization can be controlled down to the level of every business object on our platforms.

7 Transaction Security

Ensure you have native support for TLS 1.2 or above encryption and run-time validation of user actions. Built-in SOA framework for integration with external authorization and custom authorization rules. Application logic is carried out through stored procedures based on internally generated session ID, action ID, and object ID that are validated by the workflow engine.

8 Secure Client Data

Data masking can be utilized to hide original data in configurable fields to protect personal information, which is customizable within our solutions.

9 Logs and Audit Trails

In addition to producing logs and audit trails, make sure these logs and audit trails are properly secured, maintained for as long as you require, and are accessible for forensic investigation.

10 Data at Rest

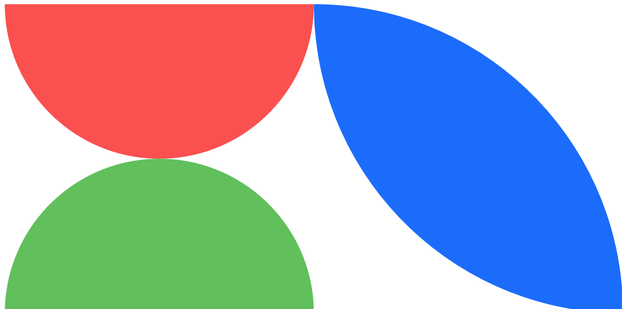
Data at rest or data stored in persistent storage should be encrypted using the Advanced Encryption Standard (AES).

11 Key Management

With native integrations to industry-leading key management solutions, be sure to have secure keys and tokens to protect sensitive data.

12 Firewalls

Implement Web Application Firewalls (WAF) and Next-Generation firewalls with an enhanced level of filtering and control. Intrusion detection systems (IDS) and intrusion prevention systems (IPSs) can monitor all traffic to and from the application.



13

Latency

Worldwide data center support for implementation allows for lower latency globally while meeting region-based regulatory requirements.

14

Regulatory Requirements

Regulators worldwide are hyper-aware of data threats and are placing increased demands on the industry. Staying abreast of pertinent existing and changing regulations strengthens our security strategy.

The OneShield Perspective

Since its inception, OneShield has maintained that security is paramount to providing exceptional solutions for insurance providers.

Through the solution delivery process, we work with our partners to provide world-class applications and infrastructure that allow our clients to rest easy and focus on the business of their business.

As a software vendor, it is our priority to secure our environments, data, clients, and employees.

We also develop our software products to abide by and support robust security practices. At OneShield, we embrace a security culture, employing a level of process to the organization and continuously introducing new, improved methodologies and solutions to align our security practices with customer requirements and industry standards. Company-wide training programs for all employees are standard, and conducting unannounced security tests randomly throughout the organization, keeps our employees well-versed in recognizing the latest threats.

From a development perspective, we continue to educate and implement controls that allow developers to find vulnerabilities or design issues early in the process to support secure coding standards and quick remediation.

Conclusion: Security Empowered Clients

The flexibility of our solutions allows OneShield to adapt very quickly to changes in the dynamic cybersecurity environment, including changes to regulations and privacy laws. Whether it is a workflow change to address concerns of the California Consumer Privacy Act, new object encryption based on expanding private data definitions, or substantive change to the overall market environment, OneShield's platforms provide the tools necessary to adopt rapid change.

There are many considerations when approaching your core system transformation. Security is one of them, but it should not steer your organization away from cloud solutions employing SaaS systems. OneShield's SaaS solutions enable insurers to rapidly propel business operations, increase overall productivity, and meet the ongoing demands of business operations with greater efficiency.

OneShield®
Cybersecurity Series

About OneShield Software

OneShield provides business solutions for P&C insurers and MGAs of all sizes.

OneShield's cloud-based and SaaS platforms include enterprise-level policy management, billing, claims, rating, relationship management, product configuration, business intelligence, and smart analytics.

Designed specifically for personal, commercial, and specialty insurance, our solutions support over 80 lines of business. OneShield's clients, some of the world's leading insurers, benefit from optimized workflows, pre-built content, seamless upgrades, collaborative implementations, and pricing models designed to lower the total cost of ownership.

Our global footprint includes corporate headquarters in Marlborough, MA, with additional offices throughout India.

For more information, visit OneShield.com