Attacks on applications are among the most costly incidents organisations can face. One coordinated attack reportedly stole US$1 billion from 50 different companies.¹

As the information explosion continues, applications are proliferating and becoming increasingly diverse – moving from mainframes and servers to clouds, smartphones, wearables and other devices. The ability to create applications, once exclusive to vendors and in-house programmers, is now commonplace.

Modern applications are written in multiple languages and run on myriad devices. Organisations no longer have the luxury of managing a handful of applications. Today’s portfolios contain thousands of diverse applications that complicate lines of responsibility and introduce unknown risk.

Complex application portfolios provide fertile ground for a growing number of vulnerabilities. Attackers know that vulnerable applications open doors into organisations’ protected systems and most valuable information: more than two thirds of attacks are targeted at applications.² Organisations that do not secure their applications present themselves as easy targets.

Good practice to reduce the risk of attacks is available, and it works. But application risk needs to be governed effectively, otherwise good practice will be applied inconsistently across the application life cycle, leaving risk unmanaged.

The ISF Application Security Framework has been developed to help organisations improve security at all stages of the application life cycle. The framework is a structured and comprehensive set of 27 good practice guidelines, derived from leading practice, expert input, standards and other guidance. The framework is supported by an iterative approach that ISF Members can use to address immediate risk and incrementally improve information security across their application portfolios.
APPLICATION SECURITY – Bringing order to chaos

HOW SHOULD ORGANISATIONS RESPOND TO INCREASING APPLICATION RISK?

By performing successive iterations of the improvement cycle shown below to:
- address immediate application risk
- incrementally improve the security of their application portfolios.

1. DEFINE
For a specific group of applications, assess current practice against the framework to determine gaps. Create and agree an implementation plan.

2. IMPLEMENT
Execute the plan to implement good practice and address the identified gaps.

3. EVALUATE
Determine the extent to which improvements and address the identified gaps.

4. ENHANCE
Identify and incorporate lessons learned to enable sustainable improvements.

THE ISF APPLICATION SECURITY FRAMEWORK

GOVERNANCE:
- Application Security
- Application Risk Management
- Application Register
- Application Ownership
- Application Security Education and Training

REQUIREMENTS:
- Application Security Requirements
- Application Security Architecture
- Application Security Policies

DESIGN:
- Application Security Design
- Application Security Approvals
- Application Security Risk

DEVELOPMENT:
- Application Security Development
- Application Security Code
- Application Security Testing

DEPLOYMENT:
- Application Security Deployment
- Application Security Environment
- Application Security Operations

OPERATIONS:
- Application Security Operations
- Application Security Monitoring
- Application Security Incident Management

DISPOSAL:
- Application Security Disposal
- Application Security Audits
- Application Security Contingency

APPLICATIONS PROLIFERATE

Organisations are not keeping up

The equivalent of 106 YEARS of downtime was suffered by Microsoft, Yahoo! and Google services in 2014 due to 11,944 outages

Only 37% of applications are tested for vulnerabilities (as of Nov 2014)

1 BILLION personal data records were compromised in 2014

ABOUT THIS REPORT

This report describes how application risk is increasing and why managing the risk is now critical, given the impacts organisations are experiencing and their reliance on applications. It highlights a number of areas that ISF research found to be particularly important in overcoming the barriers to effective application governance and risk management. Leading CISOs ensure clear governance structures are in place. They communicate across multiple organisational levels, allowing stakeholders to visualise responsibilities clearly and understand the true extent of the risk. They facilitate skills development for those who need it, in particular application teams and risk managers.

The ISF Application Security Framework, shown on the left, is the centre of the ISF approach to addressing application risk. This structured and comprehensive set of 27 good practice guidelines, shown below, is aligned with the ISF Standard of Good Practice for Information Security and will help organisations improve governance and risk management across the application lifecycle.
Application Security – Bringing order to chaos equips ISF Members to improve governance and risk management across the application life cycle. It does this by:

– articulating the magnitude of application risk
– providing practical guidance on how organisations can overcome operational barriers with clear governance, better communications, the right skills and actions to address immediate risk
– setting out an approach that incrementally improves application risk management and embeds good practice across application portfolios.

Central to the ISF approach for protecting applications and the information they handle is the ISF Application Security Framework. The 27 good practice guidelines that make up the framework are aligned with the ISF Standard of Good Practice for Information Security and a wide set of good practice including BSIMM, ISO/IEC 27034-1:2011, Microsoft SDL and SAMM.

ISF Members will also find that this report complements the ISF Information Risk Assessment Methodology 2 (IRAM2).

The ISF encourages collaboration on its research and tools. Members are invited to join the active Application Security group on ISF Live (https://www.isflive.org/community/process/application-security), to share their experience and debate findings in this report. Please let other ISF Members know how you have translated the guidelines into effective controls to improve information security across your organisation’s application portfolio.

The report is available free of charge to ISF Members, and can be downloaded from the ISF Member website www.isflive.org. Non-Members interested in purchasing the report should contact Steve Durbin at steve.durbin@securityforum.org.

2. Gartner Security and Risk Summit, 23-26 June 2014, National Harbor, Maryland, USA.

Reference: ISF15 09 02 | Copyright © 2015 Information Security Forum Limited | Classification: Public, no restrictions