STEVE JUMP

CONSULTANT

Custodiet Advisory Services

Steve Jump has an unashamedly technical background, being both a chartered engineer, and an entrepreneur, skills he uses it to translate complex technology into serious business value.

He presently consults, coaches, and advises in the field of Information Security Risk and Governance, where he expresses support, sympathy, incredulity and fortunately, frequent flashes of inspiration around the state of Information Security risk management in business today.

With over twenty years of practical and strategic information and cyber security experience. Steve provides applied cyber security risk governance coaching, mentoring, and guidance at an Exco, Board and ISO level to ensure that non-technical and technical directors alike are able to understand that information security risk is about business success more than technology, and how this understanding adds significantly more value to a business as an enabler than a fear based approach.

CISO Alliances

Holistic Fraud Framework

Inclusion of Crime & Fraud Management into the cyber threat domain

This is a cyber security perspective on mechanisms to minimize fraud opportunity, and to increase opportunity for early fraud detection.

"Much focus is given to malware and brute force cyber-criminal activities but many of the vulnerabilities that enable such actions are equally accessible to internal and external fraudulent use of the same vulnerabilities."

A majority of identified fraud in business platforms is based on obtaining unauthorized access to systems that allow unexpected actions or combinations of to be performed. These same authorization vulnerabilities are also at the root of many of the biggest cyber extortion or cyber breach events.

Such fraudulent actions may happen at a customer level or at an employee/trusted partner where the fraud is materially targeted at the hosting service provider, or to its customers or partner service providers.

The following are three perspectives based on current cyber threat reduction principles that have the potential to reduce system errors or oversight that enable fraudulent activities and to facilitate early detection of such activities.

Software Development

Secure Software Development Lifecycle (SSDLC) and Secure Software Development Frameworks (SSDF) are very much the trend after a series of extremely public breaches that were due to deliberate compromise of source code for the purposes of cyber-crime.

Such opportunity to include bypass or backdoor code is well understood, but even recently was often not seen as a primary driver to include extra preventive steps in the business application development process.

The need to prove that your inhouse/custom/purchased software was securely developed, has no malicious or unlawful content, and is still vulnerability free while in use is leading to the deployment of a variety of software development and lifecycle code provenance initiatives.

Initiatives that can greatly reduce developer level cyber threats and accidental vulnerabilities, and additionally allow improved visibility of fraudulent activity.

Indeed many of the initiatives to prevent abuse of the code development process have many similarities to those intended to prevent fraud within normal business processes.

"Such secure software frameworks have a potential not just to reduce or prevent coding error driven vulnerabilities, but with minimal extra effort at the test specification stage for cyber threats can also include the effective monitoring and alarm mechanisms for fraudulent identity and authentication processes."

ALLIANCES PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES

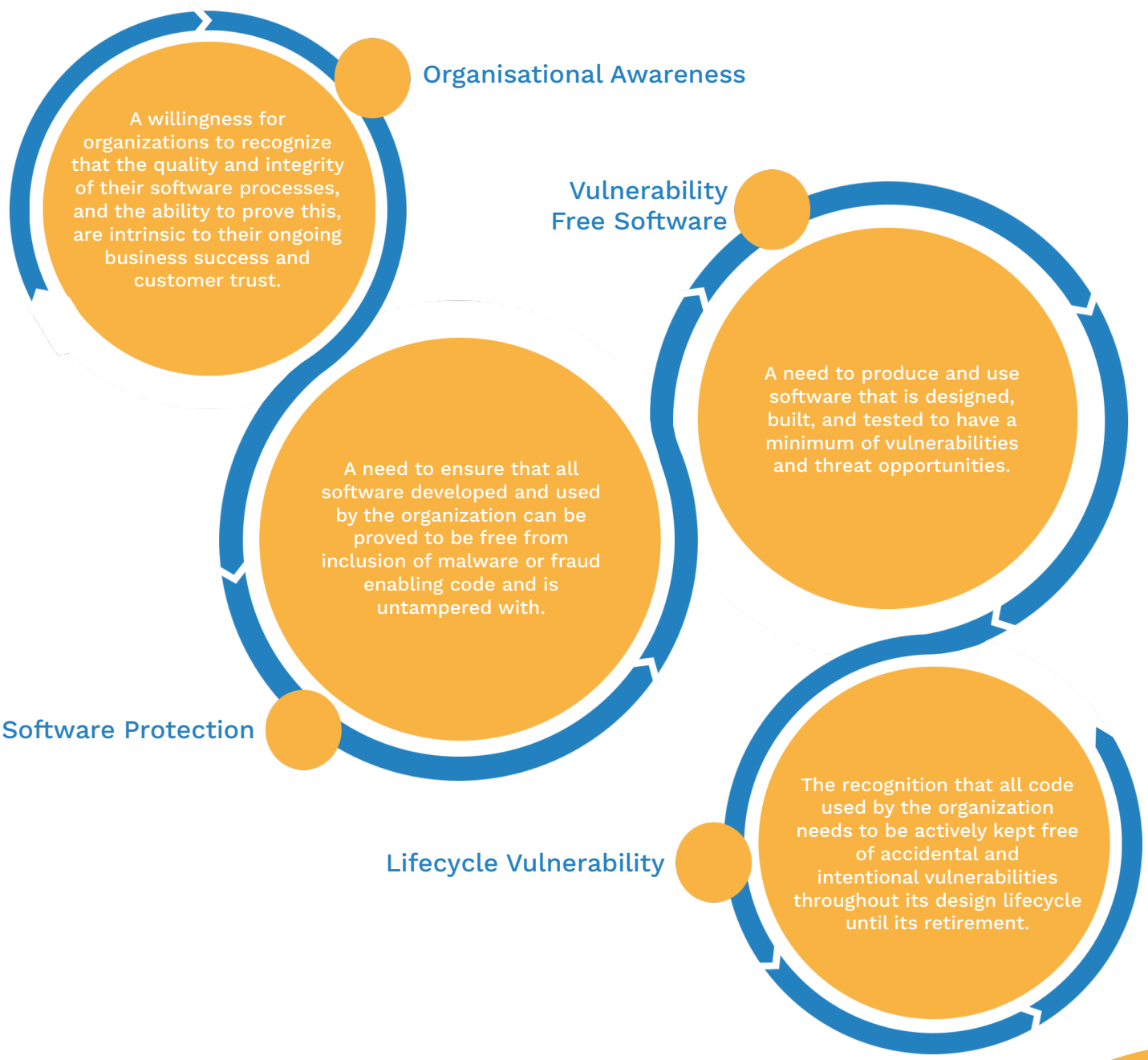
Alliances FRAMEWORKS
FRAUD & CRIME MANAGEMENT FRAMEWORK

CISO Alliances

Holistic Fraud Framework

With appropriate scoping, and the recognition and inclusion of business fraud within the cyber threat evaluation stage, applications themselves can easily be adjusted to include the identification of data and information access that has manually bypassed the conventional application access mechanisms.

Secure software development frameworks, in this case I am paraphrasing NIST SP 800-218 as an example, have four main stages that need to be addressed.



ALLIANCES PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES

Alliances FRAMEWORKS
FRAUD & CRIME MANAGEMENT FRAMEWORK

CISO Alliances

Holistic Fraud Framework

Authentication/Authorization

In the most serious cyber incidents the root cause is often directly linked to a compromised authentication token, or a broken or poorly managed authorization framework. These same technical and procedural gaps are also at the root of a majority of organizational fraud events.

"In new systems it is essential that by design an unidentified or unauthorized transaction cannot take place. With legacy apps that are often integrated with older software using shared identities it is necessary that all such transactions are logged and analysed."

New systems must adopt basic secure design principles that specifically include both enforced identity and authorization processes, ideally built into heavily protected and tested API frameworks that include error and fraud based event reporting – not just transaction success/fail.

Where older applications require human intervention all access to those applications must be engineered to take place through identity secured gateways. This is a basic for cyber risk management, and may simply be extended to cater for fraud event monitoring.

"All failed, irregular, or repeated anomalous identity events must be treated as security events, and any use or attempted use of locked identities automatically flagged."

As with all identity controls a business must not treat them as simply a faulty IT process, business must be taught not to accept default resets in any environment where fraud is possible.

UEBA – User and Entity Behavior Analysis

If identity events are not logged the forensic process to trace a loss or fraud becomes impossible. The inclusion of richer data in identity, access, and authentication events by the use of mandatory pre-configured authentication self reporting APIs can help.

But the most powerful cyber security principle that can be readily adapted to a front line fraud detection mechanism is that of User and Entity Behavior Analysis, where successful and failed events are mapped at the time of collection against a user's historic behavior, to other identical roles doing the same job, and to recognized and machine learned fraud signatures.

In exactly the same way that such tools are used in first line cyber threat detection in advanced SIEM tools. Collection of meaningful event data is a good first step, but active analysis as near to real-time as possible can deliver significant advantages in terms of damage limitation, and early major incident detection.

Such capabilities should be in place within any Cyber Security operations capability, and can simply be extended to fraud management – often using the same toolsets.

SD Jump
June 2023

ALLIANCES PROJECTS
UNITING STRENGTHS
EXPANDING OPPORTUNITIES

Alliances FRAMEWORKS
FRAUD & CRIME MANAGEMENT FRAMEWORK