OrbusSoftware

CIO Challenges:

Lack of Visibility Around Compliance and Security Risks

INTRODUCTION:
CIO Challenges: Lack of Visibility Around Compliance and Security Risks

What are the main concerns facing Chief Information Officers today? At Orbus Software we have identified 8 major issues that every enterprise is likely to struggle with when it comes to meeting the demands of the digital age.

It practically goes without saying, but doing business is fraught with risks. Firms have always had to contend with physical security, but the interconnected world now means cybersecurity has become the biggest threat. Internally, businesses have to deal with principal-agent problems, with unscrupulous employees, and with simple mistakes, but now there are many more regulations, more areas to monitor, and the connections between business elements mean even small mistakes can have huge impacts. Together, the management of these are grouped under Governance, Risk and Compliance, or GRC.

In this eBook, we will focus specifically on "Risk", and examine how organizations struggle to anticipate and prevent cybersecurity threats.

The average cost of a malware attack on a company is $2.4 million

Key Stats

- The most expensive component of a cyber attack is information loss, which represents 43% of costs

- Cloud-based cyber attacks rose 630% between January and April 2020

The Growing Threat to Modern Business

The Solarwinds attack. The Equifax data breach. WannaCry Ransomware. The Sony Pictures hack. The NotPetya malware. Just a small sample of the many hacks and data breaches that have taken place over the past few years, costing billions, possibly even trillions, in damage, fines, and thefts. A list of every major data breach would take up more space than this entire eBook. Between the number of attack vectors and the growing sophistication of the attackers (some of which are now government supported), it is no wonder that hacks have become so common and so dangerous.

Sprawling Systems Expose Vulnerabilities

In the eBook on spiralling technology costs, we mentioned a statistic that the average enterprise pays for more than 1500 applications. This obviously impacts upon costs, but it also highlights the challenge that security teams face. 1500 applications means 1500 additional potential weak points, in addition to vulnerabilities in internal systems. The uncontrolled sprawl of enterprise technology greatly complicates efforts to secure valuable information and protect operations.

The growth in applications also contributes to another problem, which is that a business cannot address third-party security issues. Even if a firm has very robust risk management, they can still be vulnerable simply because of a weakness in an email provider, or an operating system, or similar.

It takes organizations an average of 191 days to identify data breaches

Lack of Visibility Across the Organization

Huge application portfolios are just one part of a broader issue, which is that IT or Risk professionals struggle to have clear visibility over the enterprise. Aside from knowing the scale of the application and technology portfolios, there are still going to be problems with organizational and data silos, or with complex systems, or with duplicated or wasted information. If a firm cannot understand and know its structure, it is doomed to fail with security.

Waste and Duplication Afflict Existing Risk Management

No firm is going to approach risk management from scratch; there will always be some existing systems in place. Unfortunately, many of these systems are poorly done, wasting resources and often duplicating effort across different parts of the enterprise.

Damage related to cybercrime is projected to hit $6 trillion annually by 2021

Failure to Maintain Oversight

Let's put aside these issues and assume that a firm has managed to solve all its vulnerabilities. Even in this unlikely scenario, risks will still be a problem for the firm as standing still is not an option in the modern world. Software updates, new technologies, changes in business strategy or in personnel, or even new regulations will open up the firm to cyber security risk. Without permanent, effective oversight of risk management or compliance problems, organizations cannot hope to remain protected.

Employee negligence causes 48% of data breaches

Key Stats

- 69% of organizations don't believe the threats they're seeing can be blocked by their anti-virus software.
- On average, only 5% of companies' folders are properly protected
- 50% of large enterprises are spending $1 million or more annually on security
- 70% of security executives believe that their budgets for fiscal year 2021 will shrink

Minimize Risk and Ensure Compliance

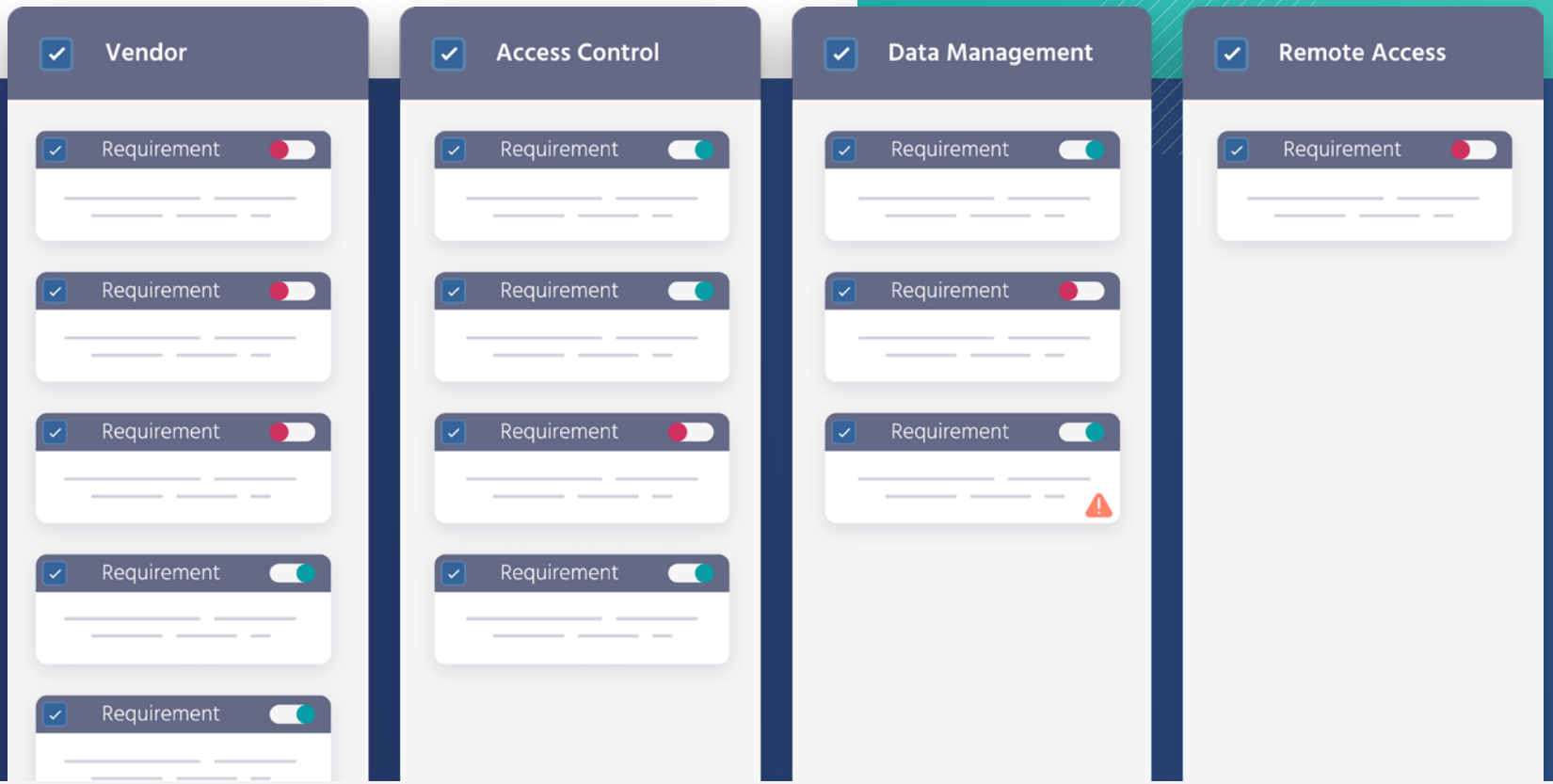
GRC is a wide and varied area that should span across the business. Any changes made to help deal with risk will cross over with governance and compliance and vice versa, which means changes made by a CIO will only be part of the overall approach to GRC for the organization. Even within the security arena, there is a difference between systems to anticipate threats, and systems to protect against threats. Fortunately, it is possible to lay strong foundations that support the whole, particularly through effective architecture.

More than 77% of organizations do not have an incident response plan

Security Architecture is the Key to Robust Defences

Security Architecture creates and maintains a unified security design that addresses risks to an organization, while being robust and repeatable. However, while it is easy to see the need for a robust security architecture, implementing and maintaining it is not simple. Architecture models require a central repository, and architects need to have visibility over the firm's entire architecture and its interdependencies. Firms can't invent effective security architectures from scratch, and so need to be able to implement common frameworks and standards.

The best way to meet these challenges is to have a well maintained enterprise architecture (EA) which security architects can use to guide them. With enterprise architecture, organizations will have existing maps and models of every aspect of the organization and relationships between them, all stored in a central repository.



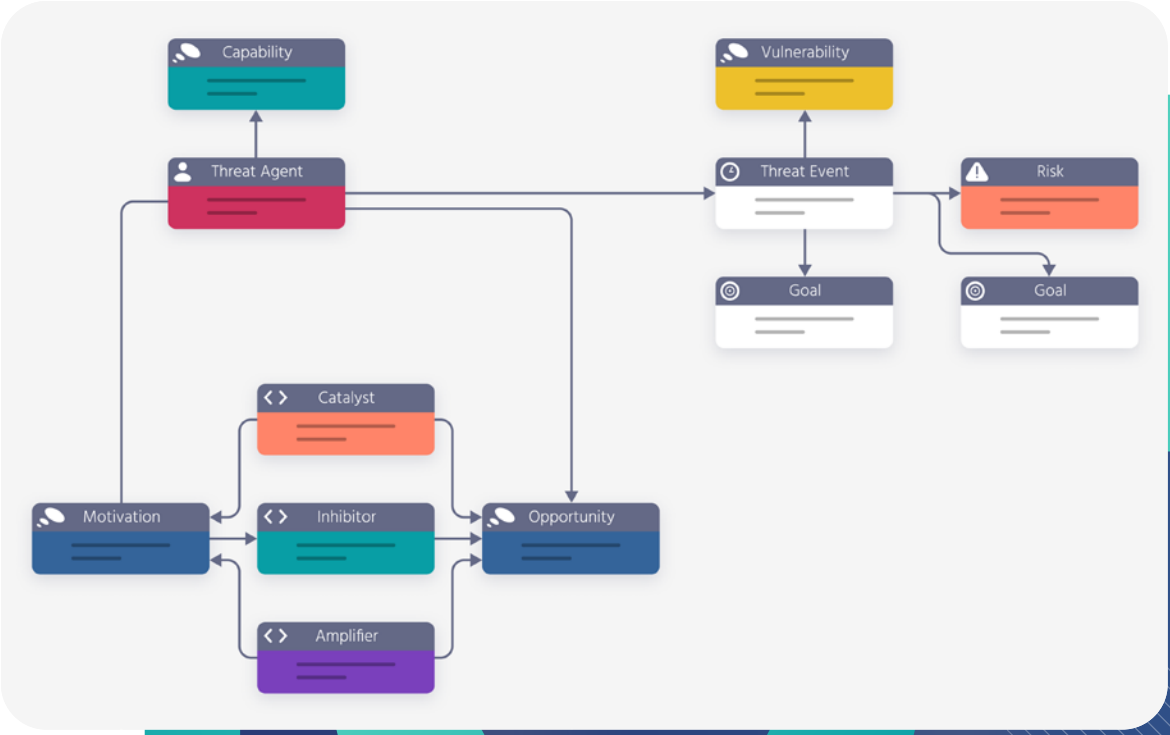
Support and Maintain the Right Framework

As mentioned above, a security architecture will typically require a security framework or standard. SABSA and the NIST CSF are two of the most widely used security frameworks and both fit well into an overall enterprise architecture. With the proper implementation of one of these frameworks into a security architecture, an organization can then apply the proper security processes to solutions that are deployed around the firm, maintaining compliance across the organization.

A Clear View of Relevant Information

Achieving the high level goals of a security architecture built on a robust framework is a great first step, but past that companies will still need to take care of the finer implementation details. One problem that plagues security architects is finding the information they need to determine how their risks or controls are associated with other elements. Most tools will be able to offer BI dashboards that can handle some of these needs, but firms will all have unique requirements. Being able to create and present custom dashboards that can deliver relevant information, with filter and search capabilities, should be a priority.

SABSA Threat Model



The iServer Suite for Enterprise Architecture: Anticipate and Prevent Potential Cybersecurity Threats

Implementing enterprise architecture and security architecture cannot be done without an effective EA tool. A good tool will provide the central repository, the modelling templates, the support for frameworks like SABSA and NIST CSF, as well as general collaboration and reporting features that enable smooth operation and communication with key stakeholders.

The iServer Suite has won Gartner's Peer Insights Customers' Choice for EA Tools for 5 years running, and was named a Leader in the EA Tool space by Forrester. Here's how the iServer Suite can provide the foresight to anticipate security threats:

A Single Source of Truth for your Enterprise

A web-based, central repository manages all enterprise content, creating a single source of truth from which security architectures can be built and maintained. Remove silos and other blockages that prevent visibility of the organization and proceed with confidence.

Address Data Redundancy and Technology Waste

Manage the removal of redundant technologies and data by identifying rarely used data and applications from the central repository. Empower cost effective security solutions without duplication.

Free Architects to Deliver Outcomes

Enable architects to deliver value through existing Microsoft365 investments. iServer365 integrates seamlessly with the Microsoft Suite, enabling architects to model in Visio and access the repository through SharePoint. Built-in support for SABSA and NIST allows the frameworks to be implemented without hassle.

Custom Views and Dashboards

iServer 365 offers a wide range of out-of-the-box views and dashboards to highlight key information and enhance security, delivered through familiar programs like PowerBI. Further, Orbus Support and Consulting services can quickly deliver custom dashboards to suit every need.

See for Yourself How To Anticipate Security Threats

Book a tailored demo today to find out how the iServer Suite helps tackle lack of visibility around compliance and security and help deal with threats

Book a Demo