Secure by Design

Research Summary

January 2022

Overview

BiZZdesign is researching the market opportunity to apply enterprise architecture techniques to cyber security risk management, to improve how cyber security risks are identified and managed. The goals of this research are to improve BiZZdesign's understanding of:

- The key stakeholders involved in managing security architecture and cyber security risks
- The responsibilities and reporting lines of these stakeholders
- The typical tasks they work on
- The goals and aspirations they have, and the challenges they face in their role
- The stakeholders they serve and the roles they collaborate with on a regular basis
- The artifacts and work products they produce
- The tooling and information they use, and interactions/dependencies with any other tooling
- How their performance is measured, including what key performance indicators are used?
- How security controls are tracked in terms of overall coverage
- How work is prioritized

Approach

BiZZdesign conducted 14 research interviews with a range of BiZZdesign customers and non-customers, whose roles are in some way directly involved in, or closely related to, cyber security risk management. These roles include:

- Chief Information Security Officer (CISO)
- Director / Senior Director of Cyber Security
- Vice President of Corporate Risk Management
- Chief Privacy Officer
- Security Architect / Security Consultant
- Chief Enterprise Architect
- Enterprise Architect
- Vice President of IT
- Senior Director of IT Infrastructure
- Head of IT Operations

The interviews were in the form of a conversation, with each interview transcribed and the transcript imported into BiZZdesign's research database where it can then be enhanced with metadata (tags) highlighting key themes and topics, to enable analysis and summarization.

Hypotheses

BiZZdesign identified three key hypotheses to be explored and evaluated in this research:

1. **Security teams are open to improve the way they work, particularly regarding collaboration with other teams**
2. **Security teams can improve their effectiveness and collaboration with improved business context for security**
3. **Enterprise Architecture tooling can improve context for security, and provide improved management information**

We believe these three hypotheses represent foundational conditions for success for Enterprise Architecture tooling to be relevant and valuable to cyber security practitioners and management, and as such represent key tests for BiZZdesign to validate continued exploratory investment in this area.

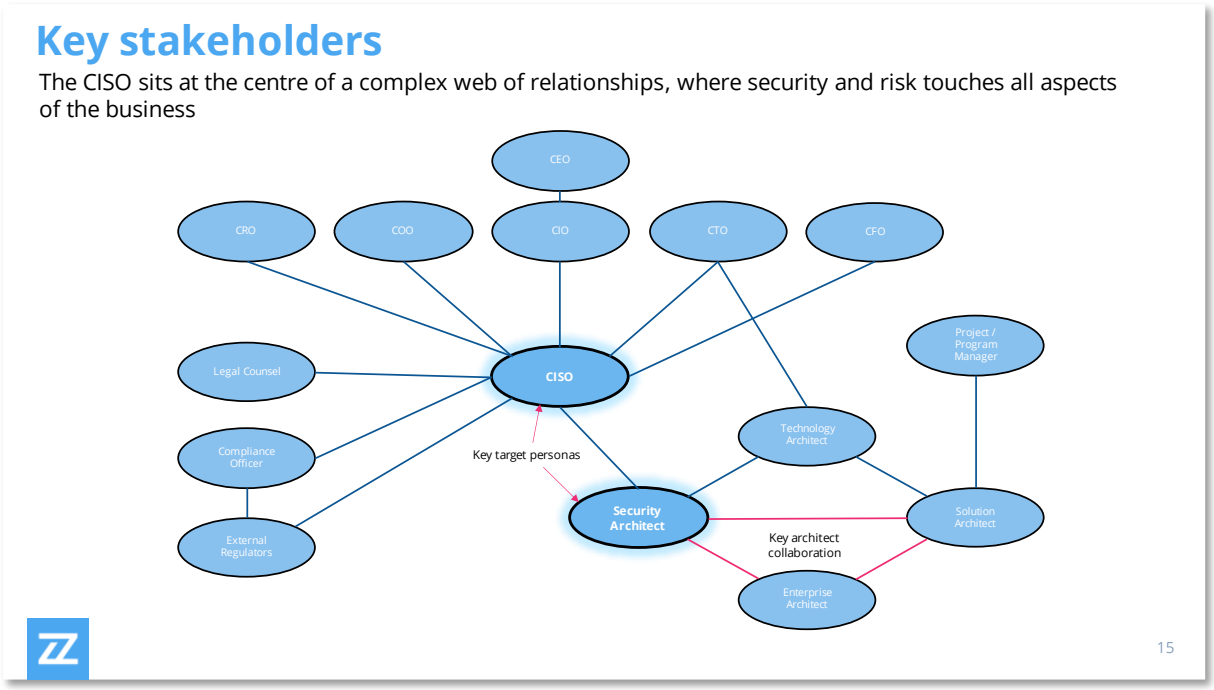
Key Findings Summary

The following is a summary of the key findings from the research interviews. Given the discussion-based nature of the interviews, it is inevitably a challenge to capture nuances of individual conversations. However, we believe these findings are representative of consistent themes that emerged from multiple interviews.

(i) Collaboration across silos is important

Security touches many teams and stakeholders, from business executives who are responsible for decision-making about risk acceptance or reduction, security teams who need to assess and advise on risk management, to development and DevOps teams who are building new solutions. When these teams cannot communicate and collaborate effectively, risks get missed.

The following diagram provides an indication of the types of roles and relationships that security teams interact with.

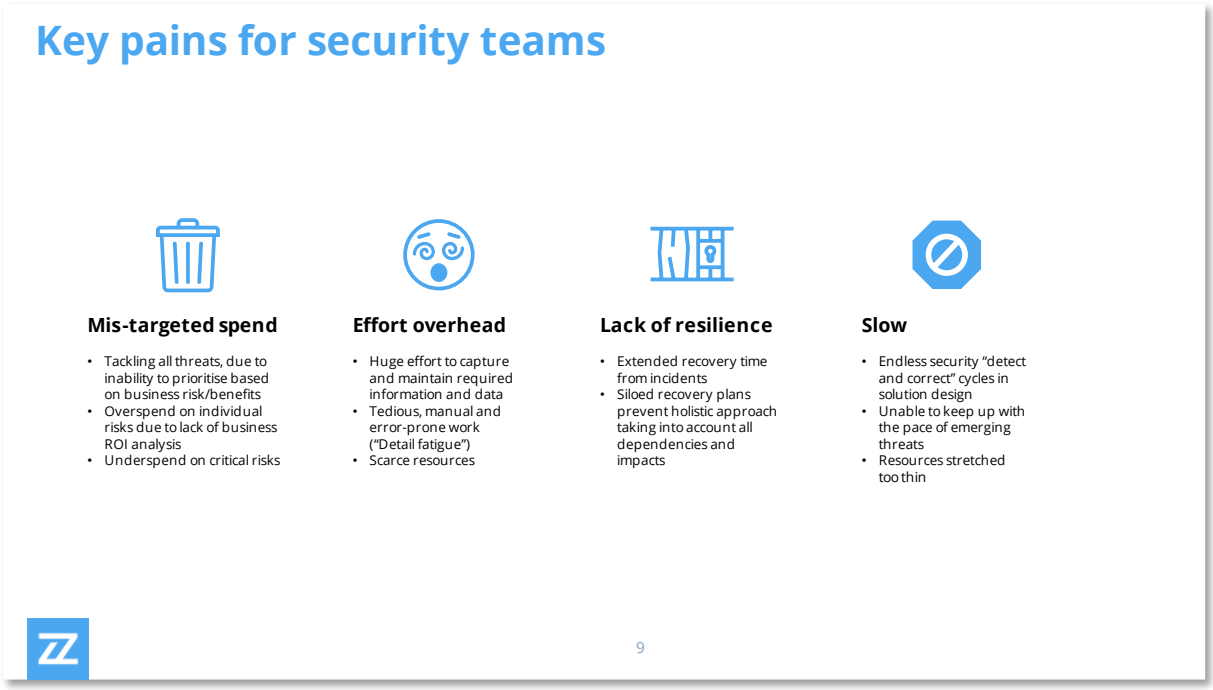


Key quotes:

- *"Security has shifted from being managed and funded as a silo… to a shared responsibility and budget between the CISO and the business."*
- *"Security is a team game. If you take a siloed approach then you're going to miss things."*
- *"It's all about being able to collaborate. You need some form of common tooling to allow these different teams to collaborate."*
- *"We typically see siloed organizations. There are separate teams for infrastructure, development, network, users in multiple remote locations, and security teams who have to stitch together the connections between all of this."*

(ii) The complexity of risks, and associated regulatory burden, is increasing

New security regulations are being published at an increasing rate by an increasing number of jurisdictions, both geographical (e.g. countries and trading blocs) and functional (e.g. industry regulators). At the same time, the complexity of security risks is increasing, due to the increasing interconnectedness and broader attack surface of digital business. And the human resources to deal with this are becoming more scarce and highly sought after.



Key quotes:

- *"There are more and more requirements to meet, in various compliance regimes, with new regulations being published almost on a daily basis."*
- *"There are new data protection and privacy rules coming out almost on a daily basis."*
- *"Having a multi-vendor environment can be an inhibitor to having a consistent, cohesive set of controls."*
- *"Operating cloud environments and legacy environments in parallel creates challenges for operating all of your security controls in a consistent way."*

(iii) Lineage and traceability between business and technology is highly desirable

Security risk is ultimately a business concern. But typically, it is a technology-centric discipline with limited visibility or traceability between the sources of risk in technology and infrastructure, the connected applications and data, and the business impacts. This impedes effective collaboration, prioritization and decision-making between business and technology stakeholders.

Cybersecurity market overview

A critical digital business enabler
Complex, fragmented, chaotic, highly technical

"Companies are recognizing that cybersecurity is a strategic priority, but they don't quite know how to get their arms around it … They don't understand how to put cyber risk in business terms."
Tucker Bailey, Partner, McKinsey

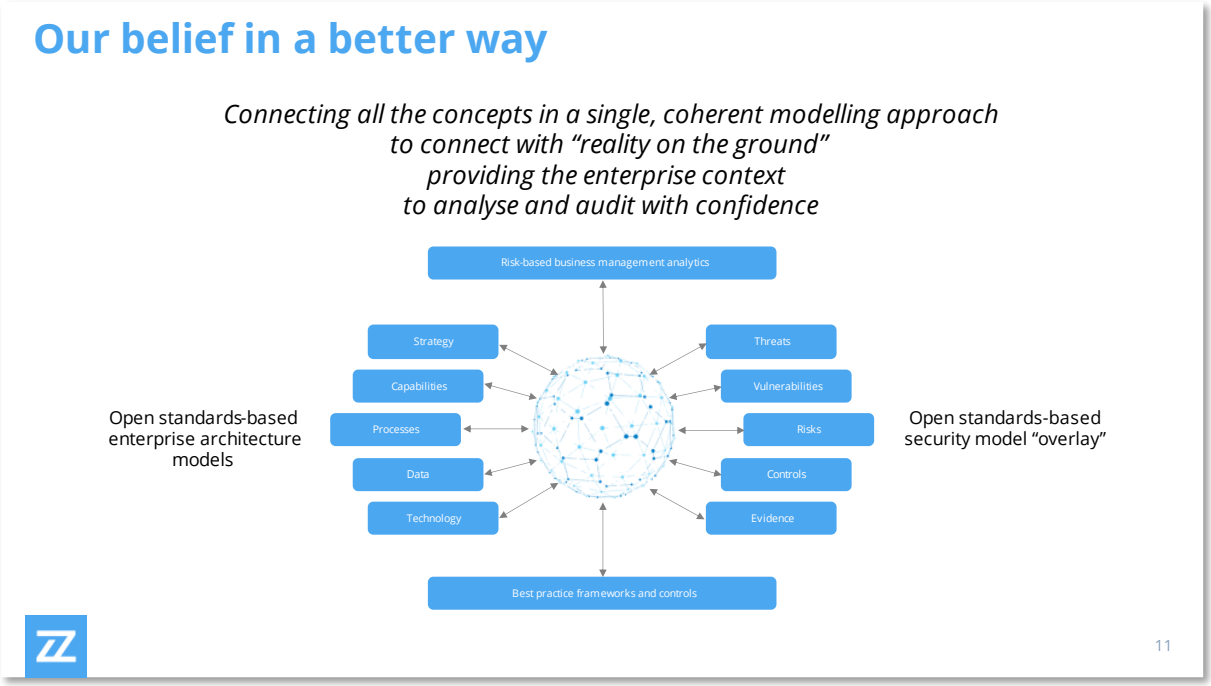
"Cybersecurity has gone beyond technology risk, for the sake of safeguarding, to a true enabler to businesses being able to move faster. But in order to realise that benefit and unlock that value, cyber has to be managed like just like any other business risk, with business leaders able to understand it and make business decisions on that risk management."
Rich Isenberg, Partner, McKinsey

Key quotes:

- *"It's kind of the Holy Grail to have the ability to trace up or down the business chain from business service to hardware. Does accounts payable go down if we experience a vulnerability in a specific piece of hardware?"*
- *"How do you know how much to worry about a threat to a technology? It's helpful to have the context to translate it to business impact."*
- *"There is definitely benefit from showing clear lineage between business controls and how they are realized practically at different levels within the technology stack."*
- *"We need to know what's out there so we can manage our technology, but also when a vulnerability is announced, or when we need to protect something, we have to understand what is connected to what, and what business service it is supporting, and how do we translate that risk?"*
- *"What would it mean for the organization should this particular asset become compromised? We want to shift left, using standard frameworks to think about the threat landscape and align that to the business criticality of the assets we're trying to protect."*
- *"If I have an incident on that server, I don't know if that server is related to the life support system. That's a problem… Incident responders need to know the inter-relatedness between different systems and their criticality and ownership… If they don't know what's connected to an incident, it hinders their ability to contain in the environment… Who do I get hold of when I need to unplug something?"*

(iv) A model-based approach enables automation, and better use of security resources

Models provide the ability to dynamically populate metrics based on queries that traverse the relationships between different connected components, provide on-demand dashboards and analytics. This provides objective, transparent insights, based on formal modelling languages and a component reuse, avoiding the overhead of manual, repetitive report creation, and freeing up expensive, scarce resources for higher value work.

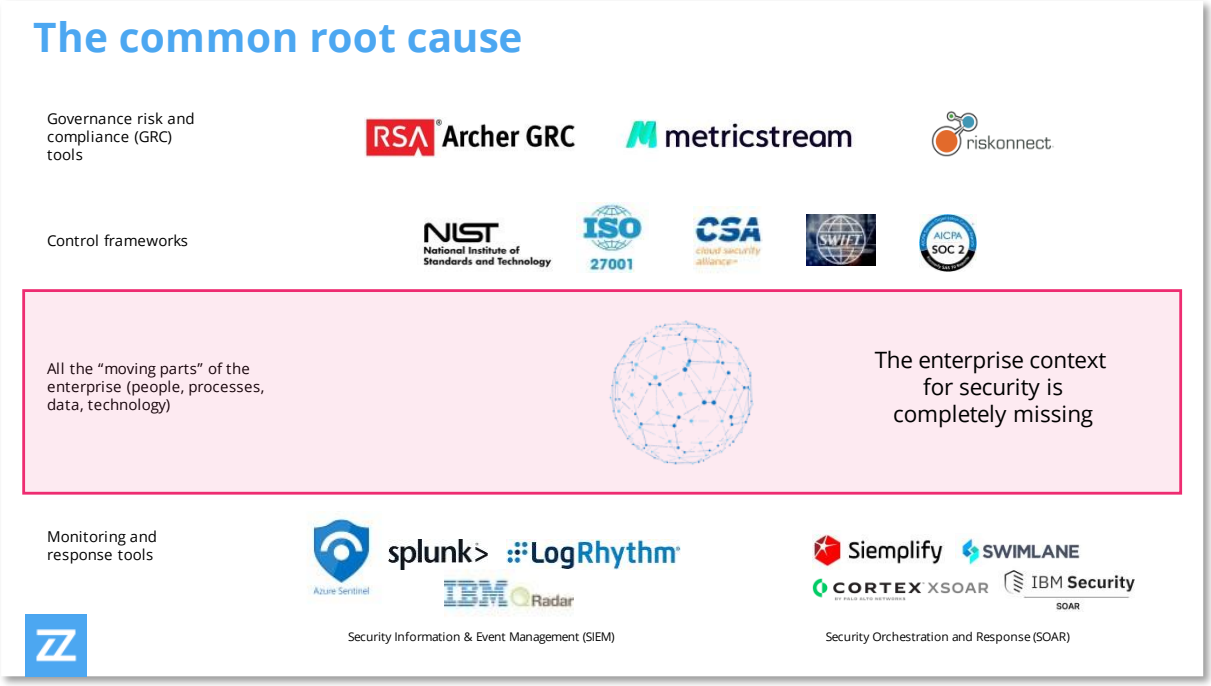


Key quotes:

- *"There are lots of benefits from using models in an automated way to evaluate adherence to standards and controls, in the same way that metrics are auto-generated in operational environments from the infrastructure, so that they can be shown on a dashboard as red, amber or green."*
- *"In a utopian world, I would like to have all our standards modelled as security controls in reference framework which you can use when you model for your particular environment… and use some form of automated reporting for objective self-assessment."*
- *"The ideal is to be able to just have a report at your fingertips that you can produce – one that will gather the data for you and produce a report."*

(v) Existing tooling is not meeting the need for improved risk context, collaboration and automation

Many security teams still use document-based approaches to documenting and assessing security architecture. Where tooling is used, it typically involves checklist-based compliance, without any business or technology context, thereby limiting the ability to truly understand and manage risk effectively.



Key quotes:

- *"You know where your assets are, you know where the threats are coming from, you know what the exposed attack surface is, you know what the attack vector might be, and that's where you need your controls. And you have to see that your controls are end to end, and have defence in depth. All that requires context. And that requires being able to physically make a map of the environment you are trying to protect. If you can't do that, you cannot start. It's like trying to play chess without being able to see the board."*
- *"I've not yet seen a GRC tool that shows any kind of contextual awareness of the thing that a risk applies to. Security is all about context… If you just have controls in a list, without context, you end up trying to apply controls that don't make any sense because they're out of context."*
- *"Our security architecture model documentation is all done in either Visio or Smartsheet, which is horrible."*

- *"We track coverage of security controls using a manual process using assessments based on spreadsheets."*

(vi) An architecture-based approach enables security governance process improvements

Performing security reviews on new applications after they've been designed and developed is becoming increasingly untenable due to the speed with which modern development teams need to iterate and release software. Creating security principles and design patterns that can be incorporated 'upstream' into development lifecycles means new solutions can be 'Secure by Design' with model-driven automation of governance processes.

Key quotes:

- *"This shift of approach helps architects to interact with other teams and provide them with requirements, best practices for compliance and governance, principles and security controls they need to consider while building their application or changing how users consume the application and data."*
- *"How do we demonstrate our controls and our ability to defend ransomware attacks? I can make up flowcharts all day long, though without the visibility that enterprise architecture provides, I can't do it justice."*

- *"There is a desire to "shift left" security in the development lifecycle… It's not about creating a new innovative value-added application and thinking 'Oh, we should secure this.' It needs to be part of the culture… To use a manufacturing analogy, it should not progress to the next lifecycle stage until the security criteria have been met."*
- *"Somebody from security was seconded into a development squad to sit with the team and practice security by design as a principle, so that security was part and parcel of that process. Similar to test-driven design and development."*

Next Steps

BiZZdesign intends to continue exploring the opportunity to apply enterprise architecture modelling and analysis techniques to improve cyber security risk management, further refining hypotheses and testing to validate or reject them.

We will also aim to identify and target specific business problems and use cases where this approach can be deployed in the form of a packaged solution, to validate market demand.

We welcome collaboration and dialogue on this topic.