IriusRisk

Digital Transformation: faster and secure

A guide to scalable threat modeling for banking and financial services organizations

The focus on digital in the banking and financial services industry is nothing new.

Now, however, the “everywhere customer” has accelerated the pace of change.

Customers expect to be able to interact with banks and financial services on any device, whenever and wherever they want—often without going near physical premises—and customer satisfaction is a competitive ‘must’. At the same time, they demand new and exciting services which continuously optimize their experience.

As a result, banks and financial services are moving ever faster towards the cloud. Service after service is becoming digital, from online and remote banking access to digital payments and cryptocurrency handling. Meanwhile, new services are continually under development. However, banking and financial services depend on one thing above all else when they digitally transform: proving to customers and partners that information and finances are fully protected.

Cybersecurity is now the number one priority.

« Security - help or hindrance

Banks and financial services companies that are going through digital transformation need to be certain that every part of the service offering, even the new launches, are locked tight. Any security vulnerability can seriously affect both company and customers.

In principle, it appears to be a simple equation. Resolve the security issues and their possible implications for the business and customers, and every form of digital transformation should be a relatively straightforward matter. Nevertheless, there are still several factors that financial services companies need to take into account.

Speed to market

Being able to capitalize on opportunity depends on speed to market. One view of security is that it slows the development and launch process down – particularly using conventional methodologies where the first touchpoint for security is testing just before release.

When security issues are inevitably identified, the business often has to make a difficult decision between releasing the software on-time but with known security flaws or delaying the release to correct the security flaws and lose a market opportunity.

Security bottleneck

In financial services, it is good security practice to include a security design review or architectural risk assessment early in the design process so that fundamental flaws in the security design are identified and can be actioned early. But there is a significant gap in the number of trained security analysts who can perform this type of review and the volume of new product initiatives clamoring for release.

This often causes the central security team to become a bottleneck in the development and release process. bottleneck in the development process.

Legacy infrastructure

Companies may not simply migrate their legacy IT to the cloud. Instead, they may choose a hybrid cloud model, running on-premises infrastructure alongside private or public cloud. This mixed environment can create an extra level of complexity that needs additional architectural security analysis.

Education

Banking and financial services companies depend on recognizing risk and assessing its implications, then taking the appropriate actions. This applies equally to software and technical security as it does to financial and business risk. Passing on expertise in security often depends on finding enough time to read masses of documents.

Regulatory compliance

In regulated industries like financial services, performing security testing alone does not meet regulatory requirements or best practice guidelines as provided by the National Institute of Standards and Technology (NIST) and Open Web Application Security Project (OWASP). Software security needs to be planned, designed and tracked all the way from inception through to deployment.

Adopting a start left approach

If security flaws and design errors are not identified until after an application goes into testing, corrections can be expensive, both in resources and in time invested. The NIST has estimated that correcting code once an application is in production can take thirty times the time required for remediation and re-design.

As a result, there has been a move towards adopting a start left approach—one that starts earlier on in the development cycle. Automated threat modeling at design time is an activity recommended by the NIST1 and the OWASP2 to ensure that engineering teams build adequate security controls into a product.

The key to scaling this activity across a large portfolio of applications is to move the responsibility for software security from the central security to the engineering teams and to empower those teams with a self-service automated threat modelling solution. This removes the central security team as a bottleneck to the product release process, allowing faster releases that still meet the security and compliance requirements of the organization.

What is threat modeling?

Modern threat modeling has moved on from manual processes. It doesn't wait until the application goes into production. Instead, it takes place in the design phase of a system or application and automates the process of threat modeling throughout the Software Development Lifecycle (SDLC), subsequently accelerating the time to market and dramatically reducing the cost of re-design. Current authorities class it as being an essential part of application design:

01.

The OWASP Top Ten calls for increased use of threat modeling, particularly when dealing with the problem of insecure design, listed as the fourth most critical security risk to applications.

02.

NIST references it as the first step in their Recommended Minimum Standard for Vendor or Developer Verification of Code.

03.

Gartner places it within the ASRTM (Application Security Requirements and Threat Management) category.

How to build a threat model

Financial services and banking organizations want threat modeling to be easy to use for everyone, and to be so well embedded in the development cycle that there’s no need to even think about it.

One typical way of building an embedded threat model is based on the basic principles of Adam Shostack’s four-question scheme. This model allows the user to detect security deficiencies during the design phase of the application.

Build the diagram

What are we building?

Pinpoint the threats

What can go wrong?

Identify the mitigations

What are we doing to protect ourselves against the threats?

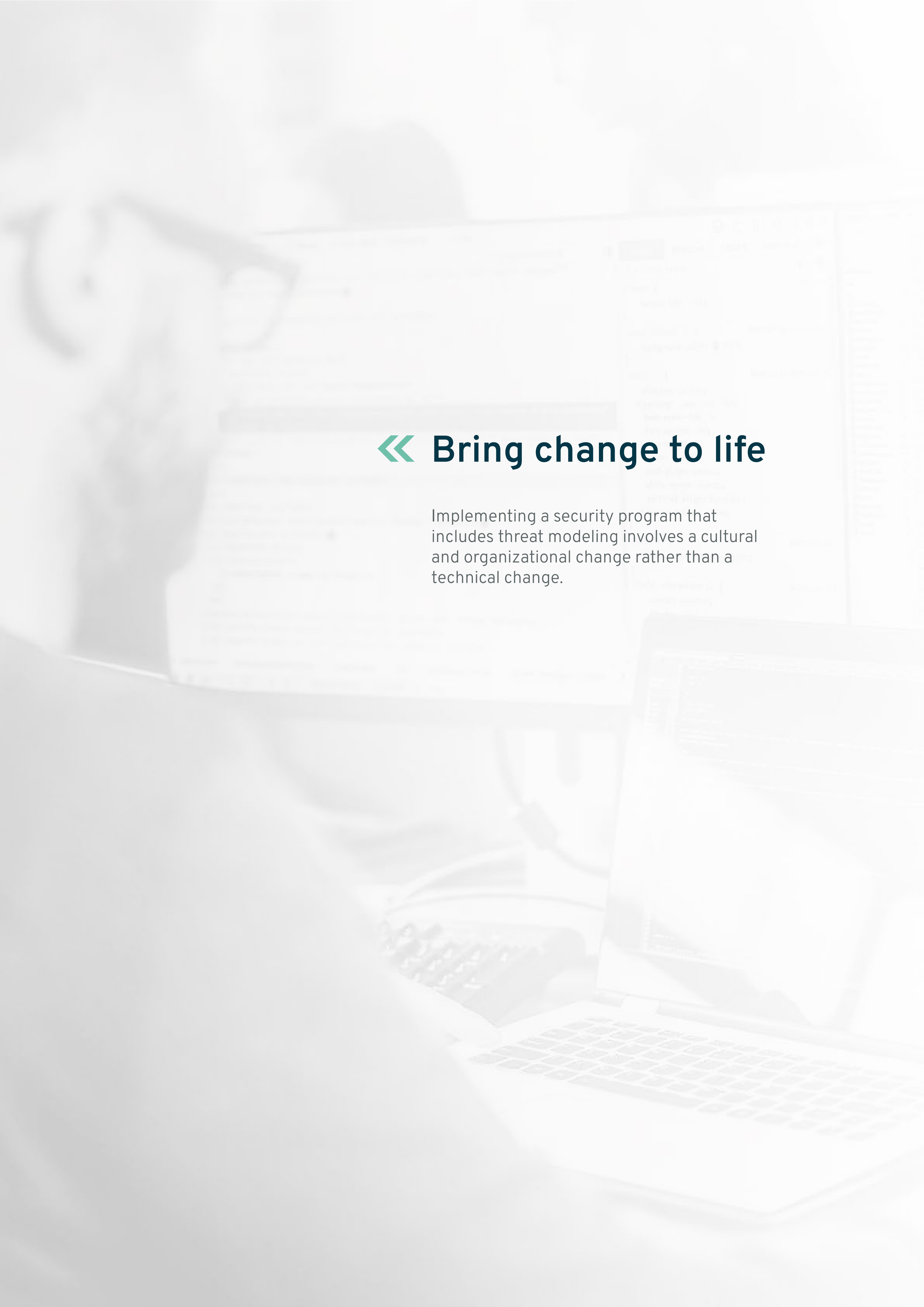
Validate the model

Did we do a good job?
Validate steps 1-3.
Document the process.

How to build a threat model

A successful Threat Modeling tool will:

- Be a single point of management for the security team. This allows them to work with an updated view of the risks within their portfolio
- Use automation to generate security requirements based on the application architecture model and the relevant standards
- Have enough flexibility to adopt either industry-specific risk models or customized security policies based on a pre-regulatory triage
- Establish a two-way communication with the Application Lifecycle Management (ALM) tools that the development teams use
- Enable API access that allows automation
- Allow dynamic updates to the risk model and implementation strategy
- Integrate with the main security tools used throughout the development cycle
- Generate a visual diagram of the architecture that can act as an active document for the mstakeholders



Bring change to life

Implementing a security program that includes threat modeling involves a cultural and organizational change rather than a technical change.

01.

Start with a pilot project that applies only to a specific set of applications to confirm there are enough resources and support to make the end result a success. Any threat modeling tool should be collaborative. This involves explaining what will take place, why it will benefit each stakeholder and what the overall effect will be.

02.

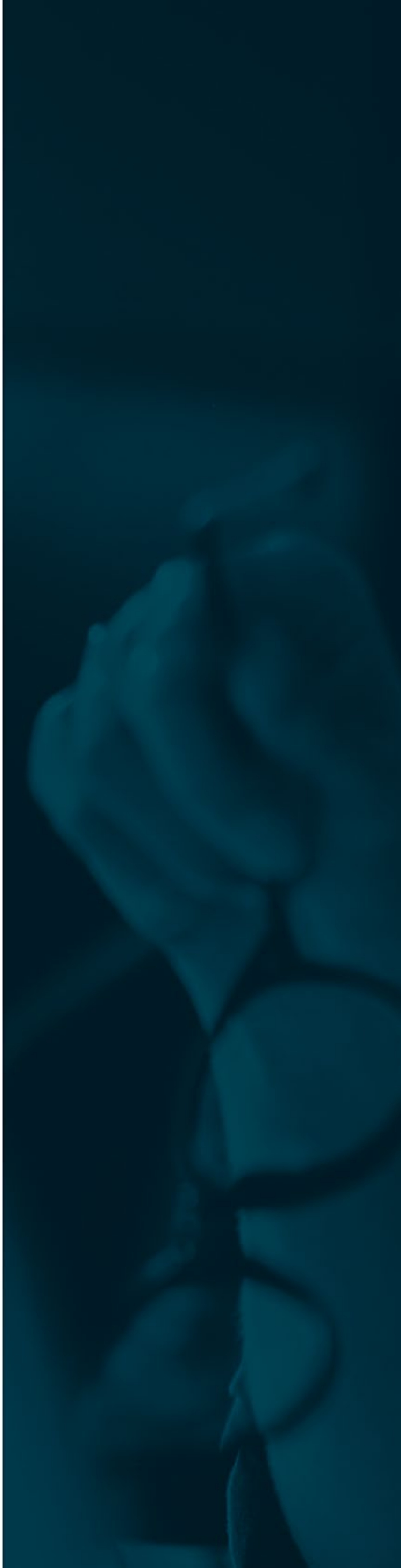
Organizational change must always be communicated, even when the project is a pilot. Adapt the corporate development procedures to include threat modeling once the application architecture is defined to make sure your project succeeds.

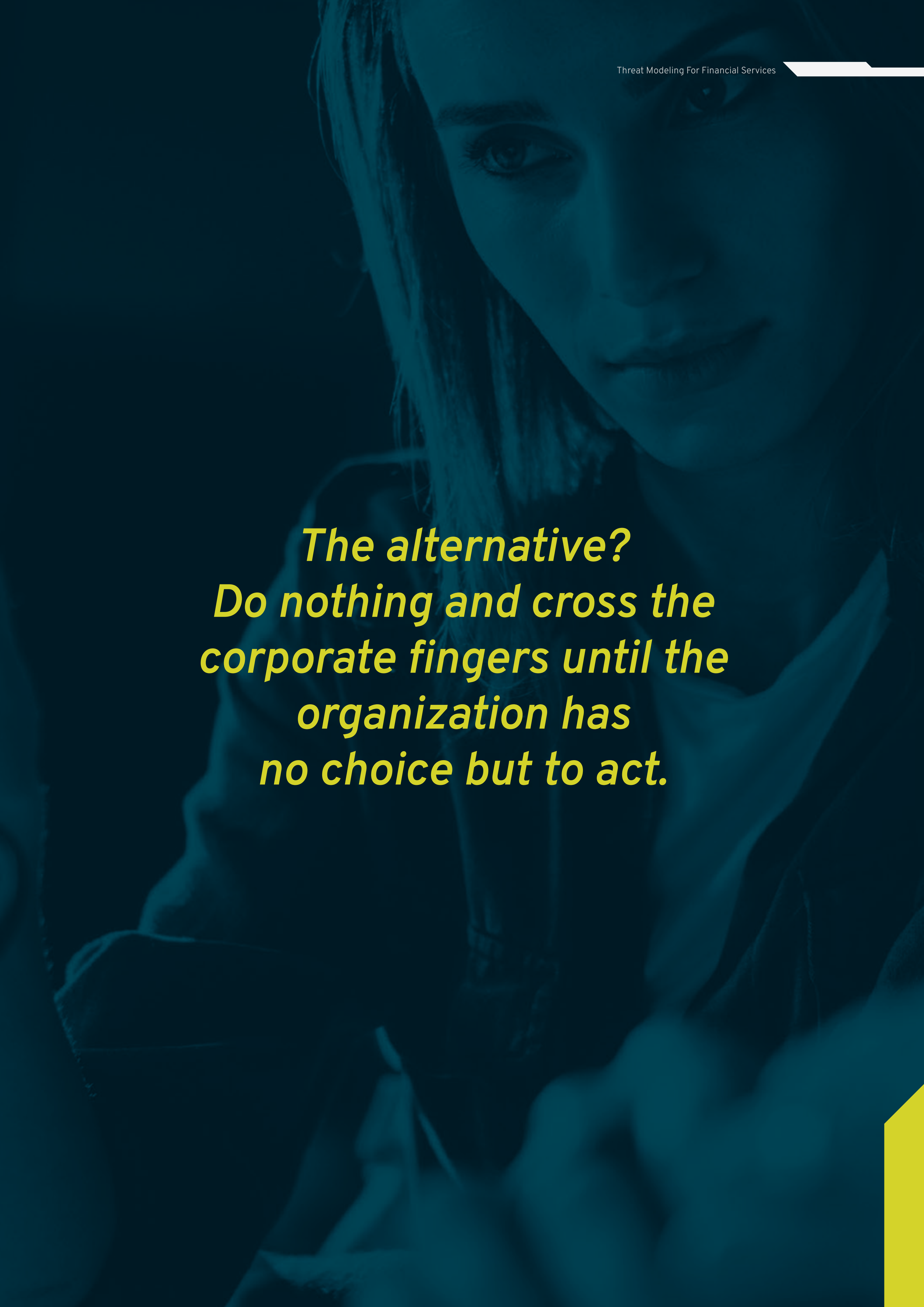
Understanding how averse to risk the business is in relation to each application is essential to creating a risk-based security strategy. A threat modeling tool helps you manage resources more efficiently so you can make better decisions.

Finally, Security Champions should remember that security requirements are not exclusively their preserve. The requirements should be published, challenged, improved and adapted to the agreed business risk appetite and regulatory compliance needs.

Undertaking a threat modeling strategy offers significant business benefits.
Not only does it present a demonstrable ROI, but it's also not a complex activity to undertake.

Threat modeling underpins other types of security testing, reviewing and auditing, and increases the productivity of business processes. It also improves time to market and instills an appetite for security all the way up to the C-suite. The alternative?
Do nothing and cross the corporate fingers until the organization has no choice but to act.





*The alternative?
Do nothing and cross the corporate fingers until the organization has no choice but to act.*

Introducing IriusRisk - Proactive software security by design

Secure doesn't have to be slow. By partnering with IriusRisk, you'll have the support of our easy-to-use automated threat modeling platform to help you identify architectural security flaws before you start building.

The IriusRisk platform can be delivered either as an on-premises solution or through SaaS. Powerful, scalable and collaborative, it's designed to help your engineering and security teams identify architectural security flaws during design, saving you time, avoiding delays and accelerating your time to market by baking security earlier into your development process.

Automated threat modelling

IriusRisk helps you beat the complexity of manual threat modeling with its powerful automation engine, providing a reliable self-service tool for designing secure applications that's simple for your engineers to use.

Security starts with design

Half of today's software flaws are in the design. Our platform lets you generate threat models in minutes, along with recommended and required countermeasures and specific, actionable advice for your engineering teams. security policies with specific, actionable advice for your engineering teams.

A smart investment

Smart threat modeling requires smart, targeted investments. Know how much to invest in security, and where to invest it, to get maximum return on your investment.

Experience our platform first-hand

Get your free lifetime subscription to IriusRisk Community Edition and start Threat Modeling within your financial services organization.

Sign up now

www.iriusrisk.com