TOREON

Threat modeling: a pragmatic guide for financial services executives

By a threat modeling trainer & developer with over 25 years hands-on experience

Table of Contents

What is threat modeling and why is it essential for financial organisations?

Think of threat modeling as a security brainstorm for your systems, before the bad stuff happens. It's a proactive, structured process to identify potential security risks in a system's design – basically asking "what can go wrong?" early on.

You and your team anticipate threats from day one.

Instead of waiting for a penetration test or (worse) a breach to reveal design flaws, you and your team anticipate threats from day one. In my 25+ years working in cybersecurity across Belgium, the Netherlands, the UK and Switzerland, I've seen one common truth: it's far cheaper and easier to build security in from the start than to bolt it on later. Threat modeling is how we do that in practice.

At its core, threat modeling comes down to four simple questions:

1. What are we building?

(Understand the system, its components and data flows.)

2. What can go wrong?

(Brainstorm possible threats or abuse cases – how could someone attack or misuse it?)

3. What are we going to do about it?

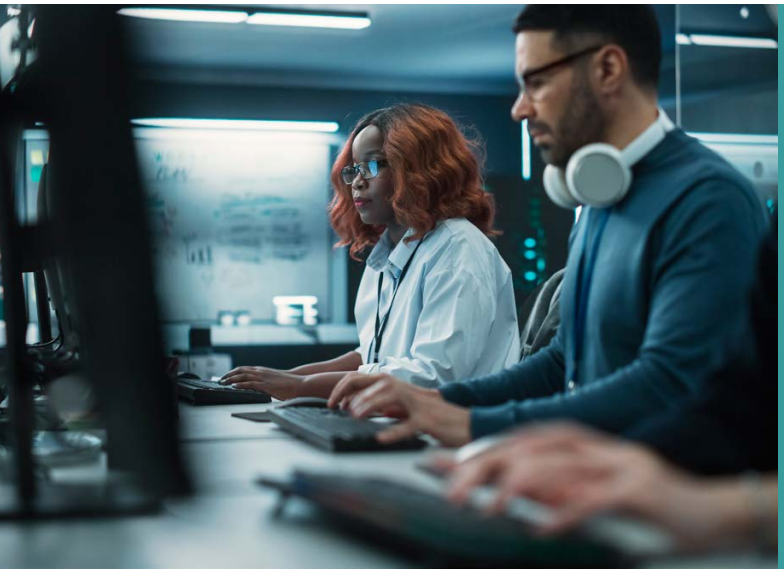
(Decide on security measures or controls to prevent those threats.)

4. Did we do a good job?

(Validate that the threats are addressed and nothing critical was overlooked.)

It's a highly **collaborative exercise**, not a solo security audit. You typically gather a cross-functional group – for example, developers, architects, product owners, even compliance and fraud experts – and map out how an application or process works.

Together, you **identify possible threats** (from technical vulnerabilities to fraud scenarios) and figure out how to mitigate them. By the end, you have a clear list of security requirements to build into the design, plus a better-shared understanding among the team.



Why does this matter for financial organizations?

Because in banking and finance, the stakes are extremely high. You're dealing with sensitive data, money flows, strict regulations, and motivated attackers. Threat modeling helps ensure that security isn't left to luck or afterthought – it becomes an integral part of designing systems and processes. Let's explore how this approach pays off in key areas like secure design, compliance, customer trust, resilience, and team collaboration.

Real-world wins: how financial firms benefit from threat modeling

Sometimes the best way to illustrate the value is through examples. While specific details are often confidential, here are a few anonymized real-world scenarios from banks and financial service companies that show threat modeling in action.

Stopping fraud before it starts

A European bank was developing a new mobile payment feature. In a threat modeling session, the team (which included a fraud analyst) identified a potential abuse case: an attacker might exploit the feature to rapidly transfer funds between accounts to game the system (basically a logic flaw to do unauthorized overdrafts). This hadn't been obvious to the developers initially. By catching it early, they added controls to detect and limit rapid transfer abuse.

Within weeks of launch, those controls thwarted suspicious activity by a malicious user. The security lead later noted that without threat modeling, that scenario likely would have been discovered "the hard way" through actual fraud incidents. Instead, it was handled proactively.

Smoother audits and less anxiety

A mid-sized financial institution underwent a rigorous IT audit as part of a regulatory compliance check (think along the lines of a DORA assessment). Thanks to their established threat modeling practice, they had up-to-date threat models for all their critical applications. They could show auditors: "Here are the top threats we identified for our online banking system and how we mitigated each."

The auditors were impressed by this level of preparation – it demonstrated a mature security-by-design approach. The firm passed the audit with flying colors, and executives had peace of mind knowing they weren't scrambling to pull together evidence at the last minute.

Efficiency gains in testing

A fintech company noticed that, after a year of integrating regular threat modeling, their penetration testing reports contained far fewer severe issues. In one case, a pen tester struggling to find major flaws actually complimented the dev team: "It's clear you guys thought about security from the start."

This wasn't just luck – the devs had a playbook of common threats (based on past threat models) that they now design against. An internal study later showed that by catching issues earlier, they cut the overall cost of security issue remediation by nearly 40%. Problems found in design were solved long before any code was shipped, avoiding costly rework and hotfixes.

Collaboration and culture

At a large bank, the CISO noticed a culture change after a year of running cross-department threat modeling workshops. Developers started inviting security team members to their planning meetings by default. Product managers began asking in early stages, "Do we need a threat model for this initiative?"

The adversarial vibe between security and development was replaced with a more cooperative spirit. One developer was quoted as saying, "Threat modeling used to sound scary, but now it just feels like a normal (and actually pretty interesting) part of how we design." This cultural shift led to faster agreement on security decisions and less pushback on security requirements, because everyone understood why they were necessary.

Customer Testimonial: Lloyds Banking

"The IriusRisk and Threat Modeling training from Toreon was a game changer. The trainers were experts, answering all our questions in a complex environment. The hands-on sessions and clear, structured approach boosted our team's confidence in using IriusRisk, whether they were beginners or experienced. It's helping us protect the bank and get more from the tool."

Maxine McFarlane, Application Security SME, Lloyds Banking Group
(Threat Model Training with IriusRisk- Toreon)

Maxine's team at Lloyds Banking Group leveraged professional threat modeling training to scale up their program – a great example of how investing in skills and tools pays off in stronger security.

Secure by design: building security in versus bolting It on later

One of the biggest advantages of threat modeling is catching issues early, when they're easiest and cheapest to fix. We've all seen projects where security was slapped on at the last minute – it's painful, expensive, and often ineffective.

I've had to help "retrofit" security into a banking app near go-live, and believe me, it's a nightmare scenario that threat modeling can prevent. By doing threat modeling during architecture and design, you bake security into the foundation.

Organizations that adopt threat modeling see their pentesters find far fewer critical issues.

Resilient by default

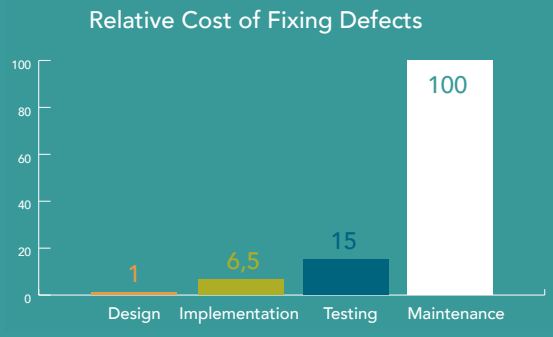
Importantly, building security in makes your systems resilient by default. If threat modeling is part of your development lifecycle, every new product or feature gets a security review at design time. You're no longer depending on QA or pentesters to catch every issue right before release. (Penetration testing is still crucial, but it becomes a validation step, not your first line of defense.)

In practice, organizations that adopt threat modeling see their pentesters find far fewer critical issues, because many were already design-reviewed and addressed. It's a great feeling to have a pentest report come back with "No critical findings" – a direct result of doing the homework upfront.

Here are the numbers

Studies back this up: according to IBM fixing a security issue during the design phase can be 30–100 times cheaper than fixing it after deployment. And those late fixes aren't just costly in Euros – they can delay launches and derail roadmaps.

A proactive "security by design" approach avoids those fire drills.



Make attackers live hard(er)

Attackers love to find the seams and cracks left in systems where security was bolted on. Threat modeling denies them those easy wins by ensuring the system's design has fewer weak links.

One European financial institution that adopted threat modeling early on found that a common web flaw (inadequate authorization for a funds transfer function) was identified and fixed at the design stage. If left unnoticed, that could have led to unauthorized withdrawals in production – a potentially costly breach. Instead, a simple design change (adding a proper authorization check) neutralized the threat long before any code was written. That's the power of being proactive.

Process before tools

Don't worry about fancy tools at the start – focus on the process and mindset. I often run threat modeling workshops with just a whiteboard or simple diagramming tool. As one bank security lead wisely said, "get the process built first, even if it's manual, and only then bring in a tool". The goal is to make threat thinking a natural part of your design culture. You can always automate parts of it later, once your team has the basics nailed down.

Compliance without just ticking boxes (DORA, GDPR, etc.)

Financial organizations face heavy compliance burdens – but threat modeling can turn compliance from a check-the-box exercise into meaningful risk management. How? By providing concrete evidence that you've considered security and privacy by design, as many laws and regulators now demand.

Digital Operational Resilience Act (DORA)

DORA expects banks and financial entities to identify and protect against ICT risks in a continuous, proactive way. Regulators don't just want to see that you have a policy; they want to see you actually implementing strong risk management in your projects.

Threat modeling directly aligns with this. It demonstrates that for each critical system, you've thought about possible threats and built in controls from the start. In fact, financial regulators and frameworks like DORA increasingly expect this level of diligence – firms should be considering threats early and often. By adopting threat modeling, you're not only checking a compliance box, but truly embracing security by design, which in turn protects your customers, reputation, and bottom line.

GDPR

GDPR mandates "privacy by design and by default." Doing a threat model can help teams surface data protection threats (e.g., how personal data could be exposed or misused) and address them upfront. When an auditor asks, "How do you ensure customer data is protected in this new payment system?", you can literally open your threat model documentation and show the identified risks (like data leakage, improper access, etc.) and how they were mitigated. This is vastly more convincing than a generic statement in a policy manual. It shows a living process rather than a paper exercise.

Financial compliance often requires performing risk assessments and showing evidence of controls. Threat modeling produces exactly that: a list of identified threats and the controls or design decisions to handle them. It's a great way to bridge the gap between high-level compliance requirements and the nitty-gritty of technical design. Instead of scrambling to do a retrospective risk analysis for the auditors, you'll have one baked into your development artifacts.

Audit readiness

Executives also appreciate threat modeling because it translates to audit readiness and easier regulatory conversations. When the board or regulators ask "How do we know this new digital banking service is secure?", you have a solid answer. You're able to say: "We conducted threat modeling during design, involving security, IT, and compliance teams. We identified these top threats and built in these specific countermeasures. We can walk you through that process." That beats simply saying "We followed policy X" any day. It shows a culture of practical compliance – doing the right things for security, not just the paperwork.

Customer trust and operational resilience: the business case

In finance, trust is everything.

Customers need to know that their bank will protect their money and personal information. One breach can shatter that trust overnight. Threat modeling plays a direct role in maintaining customer trust by reducing the likelihood of security incidents. By finding and fixing weaknesses before systems go live, you prevent those nightmare scenarios that make headlines.

Consider that the average cost of a data breach in 2023 was about $4.45 million – and that figure doesn't even fully capture the reputational damage and lost business from shaken consumer confidence. For a bank, the fallout of losing customer trust can be far worse than the immediate financial cost.

Security features conceived during threat modeling can be communicated as positives to customers.

Operational resilience

Threat modeling contributes to what we call **operational resilience**. Essentially, it means your organization can continue to operate and serve customers even in the face of disruptions (cyber attacks included). By systematically examining "what could go wrong," threat modeling helps ensure that critical systems have the necessary protections and fail-safes.

For example, you might uncover that all your transaction processing servers sit in one trust domain with no isolation – an operational risk if malware spreads there. The threat model would flag that, prompting a design change to add network segmentation or backup processes. Down the line, if a cyber incident occurs, that foresight can be the difference between a contained issue and a major outage.

Customer experience

There's also a customer experience angle: security features conceived during threat modeling can be communicated as positives to customers. Think of things like multi-factor authentication, fraud detection alerts, or robust privacy settings – these often result from identifying threats and deciding how to counter them.

When customers see these in your product, it builds their confidence that you take security seriously. In contrast, security measures slapped on awkwardly (or breaches leading to sudden new restrictions) can frustrate users. Designing with security from the get-go leads to a smoother, more transparent protection for users.

Conclusion

Preventing breaches and disruptions through threat modeling isn't just an IT win; it's a business win. It means fewer embarrassing headlines, more reliable services, and a stronger brand. In the competitive financial sector, trust and reliability are key differentiators.

Proactive threat modeling is like an investment in an insurance policy for that trust – one that pays dividends by keeping your institution off the front page for the wrong reasons.

Breaking down silos: threat modeling as a team sport

One thing I love about threat modeling is how it brings people together. In many financial organizations (including banks, fintechs, and insurers), security, IT, and business folks often operate in silos – each with their own perspective and priorities.

Breaking down silos

And in a regulated industry where security, compliance, and business agility all need to coexist, those silos can create real risk. Threat modeling sessions naturally **break down those silos**. You get developers, architects, security analysts, and even compliance or fraud experts in the same room (or Teams call), talking through the system together. All these perspectives mix, and magic happens: a developer might realize a seemingly minor feature could open the door to synthetic identity fraud or account misuse, or a business manager might finally see why a certain security control is actually crucial for protecting customers. I've seen these "lightbulb moments" first-hand, and they're invaluable.

Consensus building

By collaborating on a threat model, **everyone ends up on the same page about the threats and how to tackle them**. This consensus-building is extremely valuable.

In a bank, you often have to balance security with usability and business needs – having the key stakeholders hash it out together means you're more likely to find solutions that everyone buys into. It's no longer security versus business, or IT versus compliance; it's a shared understanding that "we either design a secure, compliant system together, or we'll all deal with regulatory and reputational fallout together". That's a powerful cultural shift.

On-the-job training

Cross-functional threat modeling also serves as on-the-job training.

- Product owners learn from security experts how hackers think and what red flags to watch for.
- Security teams learn more about the business context – what the application is supposed to do, what "normal" vs. "abnormal" use looks like – which helps them tailor their guidance.
- Developers learn how fraudsters might abuse payment flows or onboarding screens, while compliance and InfoSec learn what the app is actually doing with customer data.

Over time, this improves the security acumen of the whole organization. You'll find developers starting to raise potential threats in design meetings unprompted, or business analysts flagging data protection concerns on their own. That's when you know the silo walls are coming down.

Less conflicts

Finally, involving different teams early heads off potential conflicts down the line. If compliance is in the threat modeling workshop, they're less likely to come in at the end of a project and say "Hold everything – we can't go live because of XYZ risk." They were part of identifying and agreeing on how to handle that risk from the start. This saves time and frustration for everyone. In essence, **threat modeling injects security into the company DNA** – not as an outside enforcer, but as a collaborative partner with the business. That cultural integration is arguably as valuable as the technical outcomes.

Conclusion

Threat modeling artifacts (like diagrams and threat lists) become a communication tool. They can be shared with leadership, auditors, new team members, etc., to quickly convey "here's our architecture, and here are the main things we worry about and have mitigations for."

Instead of each department doing their own separate risk assessment in a vacuum, you have a unified view. For financial firms that are often large and complex, this unified threat picture is a game-changer. It ensures that, for example, the cybersecurity team's priorities are directly informed by what could impact critical business processes, and vice versa.

Shifting Left: embedding threat modeling early and often (and tying it into testing)

The phrase **"shift left"** gets thrown around a lot, but threat modeling is a prime example of what it really means. Shifting left is about tackling security as early as possible in the development process.

In practice, that could mean doing a quick threat model as soon as you have a high-level design or even user stories for a new feature. You don't wait until everything is built and ready to test – you start when things are still in diagram or spec form. This way, security requirements come out of the threa into the design and build phases t model and go into the design and build phases. It's much easier to add a required authentication step or input validation while you're designing a module than to retrofit it after coding.

That could mean doing a quick threat model as soon as you have a high-level design or even user stories for a new feature.

Embed threat modeling into existing workflows

A pragmatic approach many financial firms take is to **integrate threat modeling into existing workflows**. For example, during the architecture review for a new application, include threat modeling as a checkpoint. Or in agile environments, have a light-weight threat discussion whenever a new epic or user story that touches sensitive data is being groomed. It doesn't need to be a huge, formal process every time – even a 1-hour discussion can surface key threats for a feature and how to address them. The idea is to make it a habit. Every project, every significant change, think about threats early.

Combining threat modeling & pen-testing

Now, how does this tie into testing? Think of threat modeling and penetration testing as complementary. Threat modeling is **design-time analysis**; penetration testing is **run-time validation**.

If you do a thorough threat model, by the time testers or ethical hackers poke at the system, they ideally shouldn't find major design oversights – maybe some implementation bugs, but the big things (like "no one thought an attacker might do X") have been covered.

In fact, you can give the pentesting team your threat model results as homework – "These are the scenarios we think are risky; please focus on verifying these and see if we missed anything." This makes pentesting more efficient and relevant. And if the testers do find something you missed, that's great feedback to improve your next threat model. You can update the threat model with that new insight, and even add it to your secure design checklist for future projects.

By aligning threat modeling with development and testing, you create a virtuous cycle. Early modeling informs development; later testing validates and enhances the models. The end result is a significantly stronger security posture, with less chaos and surprise fixes late in the game. Developers start to internalize security thinking (because they know it's coming in design discussions), and security folks get to see their recommendations concretely implemented rather than finding issues after the fact. For a financial organization, this means smoother project deliveries and a more predictable path to securing new innovations.

Conclusion

Embedding threat modeling early has a lifecycle benefit: you keep revisiting it. Threats evolve, systems change – maybe you migrate a banking application to the cloud, or you add a new API for partners. Each time, you **re-evaluate the threat model**. It's a living document, not a one-time exercise. This ensures continuity of security.

I often compare it to a risk register that actually gets used and updated, not one that sits in a drawer. If you acquire a fintech startup, one of the first things you might do is threat model their platform to integrate it securely. If you're adopting machine learning for fraud detection, threat model that pipeline for adversarial manipulation or data poisoning risks. The process scales and adapts.

5 things to remember about threat modeling if you're in financial services

1. Threat modeling enables secure, compliant systems by design
2. Threat modeling builds confidence: internally and externally
3. Getting started with threat modelig is straightforward and scalable
4. Threat modeling is about risk reduction, not perfection
5. Threat modeling is one of the most practical tools available

1. Threat modeling enables secure, compliant systems by design

Threat modeling might sound technical, but at heart it's a business enabler for financial organizations. It allows you to design secure systems by design, not as an afterthought, and in doing so, protect the things that matter – customer trust, uptime and resilience, regulatory standing, and ultimately the bottom line.

As an executive, you don't need to know the intricacies of STRIDE or data flow diagrams; what you need to know is that your teams have a process to think like attackers before the attackers strike, and to shore up defenses in advance.

2. Threat modeling builds confidence: internally and externally

In my experience, banks and fintechs that embrace threat modeling tend to sleep a little easier at night. When your CIO asks, "Are we sure this new trading platform is secure?", you can confidently answer that you've mapped out the threats and built it accordingly.

When a new regulation comes out demanding proof of "security by design," you're already doing it. When customers ask how you protect them, you have tangible practices to point to. That confidence makes a difference – with your board, with auditors, and with the customers.

3. Getting started with threat modeling is straightforward and scalable

Getting started is not overly complex. Pick a critical project and pilot a threat modeling workshop. Bring in an experienced facilitator or use a framework your security team is familiar with.

Make it fun and engaging – a creative exercise in outsmarting hypothetical criminals.

You'll likely find it generates lively discussion and ideas. Take those outputs and feed them into your development requirements. Rinse and repeat. Over time, threat modeling will become a natural part of your organization's muscle memory.

After two and a half decades in this field, I'm more convinced than ever that collaborative threat modeling is one of the best tools we have to build secure, resilient financial services.

4. Threat modeling is about risk reduction, not perfection

Remember, the goal isn't perfection or predicting every possible attack (no one has a crystal ball). It's about systematically reducing your risk exposure and avoiding obvious mistakes. It's about being able to look regulators, customers, and your own board in the eye and demonstrate that you're doing everything reasonable to secure your systems.

For financial-sector leaders, threat modeling is a smart investment. It's not academic or nice-to-have – it's a practical approach that yields real results. As the threat landscape evolves (with new fintech, AI, open banking APIs, etc.), having this capability in-house means you can adapt and stay ahead of attackers and compliance demands alike.

5. Threat modeling is one of the most practical tools available

To wrap up on a personal note: After two and a half decades in this field, I'm more convinced than ever that collaborative threat modeling is one of the best tools we have to build secure, resilient financial services. It's grounded, pragmatic, and proven.

In a world of unpredictable cyber threats, it provides a bit of predictability – a way to not just react to the latest incident, but to anticipate and prevent the next one. And that is something every C-suite can appreciate, is it not?

Take the next step in maturing your threat modeling practice

Stay up-to-date on threat modeling

This whitepaper is part of a series of blogs, whitepapers, cases and other content that we publish on threat modeling.

Want to stay informed and know when we publish new content? Then please make sure to subscribe to our monthly Threat Modeling Insider newsletter.

We promise we will never ever send you more than one mail a week. No sales pitches, just relevant, informative and qualitative content.

Subscribe to THREAT MODELING INSIDER

Discover our threat modeling training

We offer two tailored security training options: an in-company program for teams or a 20-hour online course for individuals.

Both provide hands-on experience, expert guidance, and custom threat modeling to elevate your security skills.

Discover our TRAINING OFFERING on threat modeling

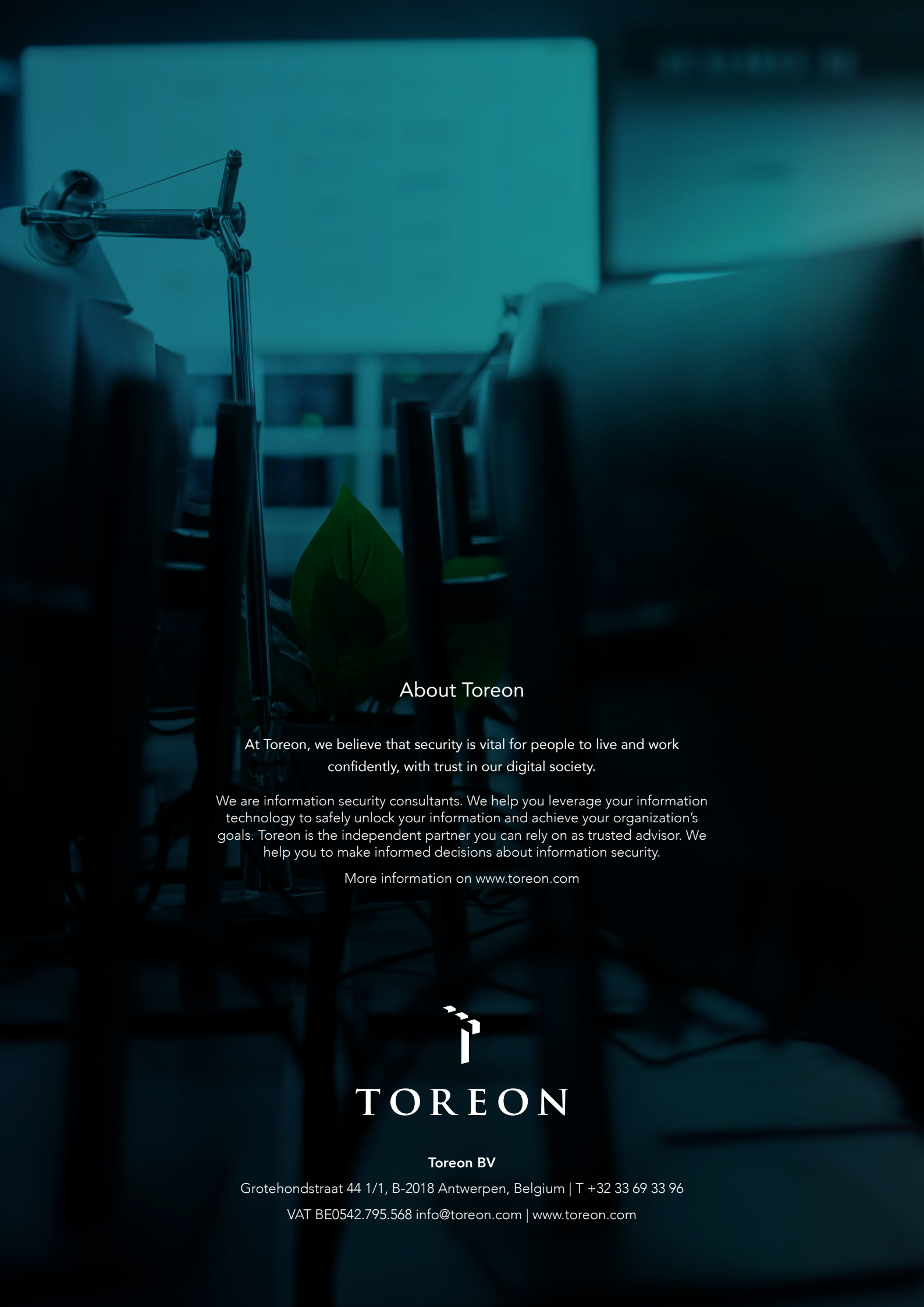
Got security-related questions?

Got specific questions on threat modeling or cybersecurity in general?

Don't hesitate to book a free call with one of our experts.

We're sure we can help or advice.

Book a free EXPERT CALL



About Toreon

At Toreon, we believe that security is vital for people to live and work confidently, with trust in our digital society.

We are information security consultants. We help you leverage your information technology to safely unlock your information and achieve your organization's goals. Toreon is the independent partner you can rely on as trusted advisor. We help you to make informed decisions about information security.

More information on www.toreon.com

TOREON

Toreon BV

Grotehondstraat 44 1/1, B-2018 Antwerpen, Belgium | T +32 33 69 33 96

VAT BE0542.795.568 info@toreon.com | www.toreon.com