How to Build a Security Roadmap

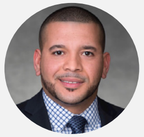
Practical advice from our CISO network

STOTT AND MAY

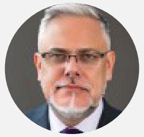
Table of **contents**

HOW TO BUILD A SECURITY ROADMAP

Guest Contributors



Brian Lozada
CISO
Prime Video



Mike Wilkes
Security Advisor
Ammolite Analytx, Wallarm & SecurityScorecard

Jessica Robinson
Founder & CEO
PurePoint International

Dan Walsh
CISO
VillageMD

Sadiq Khan
CISO
BlueVoyant

Key considerations when **building a security roadmap**

#1 Start with an external assessment

An external assessment is arguably one of the most critical phases of building a security roadmap. Think of this as a lifecycle action that needs to be completed every one-to-two years. It's an essential stage because it allows CISOs to create an agreed and documented set of risks that the business can start to believe in.

The assessment ensures that cyber security functions aren't over-allocating resources to problems that don't have a tremendous amount of weight or gravitas in the organization. Focus on acquiring a solid and reliable risk assessment to create a defined risk register to prioritize.

#2 Don't make assumptions around executive support

Executive support is an absolute prerequisite to creating a practical security roadmap. Both the business and security roadmaps need to align tightly. It's important to leverage this process of prioritization and quantifying the impact of risks as an opportunity to find gaps in your resource planning and seek out the appropriate level of funding.

Understand where your business is going within the next year. Suppose the business will pursue a new channel of customer acquisition or release new products in new markets, for example. In that case, it's important to ensure the security roadmap reflects that. There needs to be a clear mapping between the decisions you are making as a business and the focus areas of the roadmap. There's a perception that security is primarily about support, but it's also about creating or contributing towards an effective customer experience.

#3 Understand your 'business as usual'

It's important to ensure that your roadmap is realistic in terms of the resources you have at your disposal with actionable KPIs. This will allow you to demonstrate progress to the business. Ensure you go through the process of defining what business as usual looks like for your team. Whether providing design architecture support to the business or investigating incidents as they arise, a lot can distract from planned activity. This workload needs to be tracked over time to ensure the volume of commitments you make are achievable. Work towards identifying the ideal percentage of time to allocate to projects versus pure operational support.

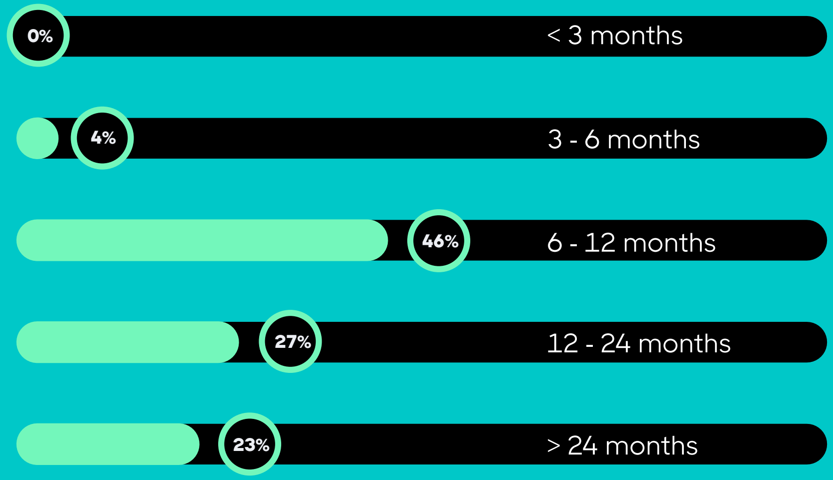
#4 Make sure your roadmap is targeted and timed

There's a bit of debate around the duration a security roadmap should cover. It's likely to depend slightly depending on the size and sector of your business. For example, in a large, established financial services business with a large amount of corporate governance, you might be able to set out a roadmap for 2-3 years. In startup environments, however, onboarding a new customer may completely reshape the security roadmap overnight.

When we asked 50 security professionals what the ideal duration of a roadmap should be, the majority (46%) stated that 6 months to a year would be optimal. Only 4% opted for 3-6 months, 27% stated 1-2 years and 23% preferred to build roadmaps for 2 years and over. "There are no right or wrong answers. It's worth aiming for around 6 months of detailed project plans, goals, and objectives for the year. This approach provides flexibility to evaluate new business priorities as they arise. Try to set expectations for potential shifts and maintain a contingency fund of approximately 8-10% to cover unexpected incidents and new critical projects that may arise along the way," one CISO stated.

Make sure your plan is targeted, giving thought to trying to quantify the answer to the question, 'How secure are we?' This will allow you to ensure that your investment reduces risk more tangibly and could culminate in a scorecard informing your narrative to the board.

What is the ideal duration of a security roadmap?



(Based on the views of 50 security leaders.)

FEATURE

Practical tips for building a **security roadmap**

Jessica Robinson
Founder & CEO
PurePoint International

Purepoint International is a boutique security firm helping businesses, including insurance companies, financial services firms, law firms, health services, social enterprises, international non-profits, and women-founded, owned, and led businesses, prevent data breaches. Under Jessica's leadership, Purepoint International has become the number one security company for women-owned and women-led enterprises globally and was recently awarded the JCI Philippines-New York ICON Award for International Affairs and Women's Security. We recently sat down with her to discuss the importance of building an effective cyber security roadmap.

Q. Why is it important to have a clear security roadmap?

Setting clear security objectives that align with the wider business objectives is fundamental to any security function's success. These objectives must be clearly communicated via a security roadmap, including the security team and the wider business. For a roadmap to be effective, it needs to be understood by business leaders within the organization, whether they have a security background or not.

It becomes very difficult for you as CISO to clearly articulate what you want to achieve and get buy-in from the senior leadership team without a clear plan in place. It is also easier to communicate when something is achieved or to show the true impact and value of the cyber function with a roadmap. Continuing to show value is absolutely essential to securing future investment in the cyber security program within your organization.

The changing regulatory landscape has also become an accelerator behind why it is essential to have a roadmap in place. Smaller companies and organizations across almost every industry are now required to comply in ways they have never had to before. Regulation drives action, and any action needs to be adequately scoped with the appropriate resources allocated as part of a broader roadmap.

Q. How important is it to understand your security posture accurately before creating a roadmap?

It is crucial to understand the security environment of the business before creating a roadmap. Typically, this is done through conducting a risk assessment and reviewing other supplementary documents, including audits or previous risk assessments. However, at the end of the day, depending on where the company is in its lifecycle or the length of time one has been in the CISO role, you can't know everything. You will need to modify the roadmap along the way - ensure there is a degree of flexibility in your plan.

The most successful companies are the ones that have a comprehensive enough roadmap that supports the long and short-term objectives of the business and one that can be adjusted and adapted. The business, technology, and regulatory landscape is changing constantly, and a good roadmap needs to be able to adapt to those changes. As CISO, you need to have a long-term vision but stay agile at the same time. A good security roadmap should be able to respond to regulatory changes and short-term threats to the business, so flexibility and agility are crucial while remaining focused on the long-term goals of the company.

Q. Which stakeholders should you make sure you consult along the journey of creating a roadmap?

The first step is forming a risk committee comprising your security team and the wider business units, including risk, finance, legal, compliance, marketing and communications, HR, and IT. It should be a multi-stakeholder group of people from across the entire business. As CISO, you need to influence the whole organization, so leaving people out in the early stages could cause issues down the road.

Once you have gathered feedback on the roadmap from the risk committee, it is time to take it to the next level and get buy-in from the senior leadership within the organization and, of course, the board. To get this buy-in, your security roadmap needs to clearly align with the business objectives and outline what will be achieved over a 12-36-month period from a security perspective to help reach those goals.

Q. How can you ensure that your roadmap aligns with business objectives?

The most important factor in ensuring your roadmap aligns with business objectives is canvassing the views of your senior leadership team. Getting that buy-in comes from the very top, so ensuring your CEO is invested in your security roadmap and understands the implications if the plan is not supported is critical to your success as CISO. That may mean you first need to educate the CEO and the wider leadership team about how a cyber security breach would really impact them. A lot of companies only act after a breach has already occurred. The goal would be to avoid this situation at all costs.

When the CEO and broader leadership understand the implications of not meeting specific security objectives (e.g., regulatory compliance, vendor risk), they will become much more invested in the security function and what you are trying to achieve. Once they understand your roadmap and its importance, it is about holding them accountable for achieving those objectives. Creating accountability is a difficult conversation to have with your senior leadership team, but it is vital to your success as a CISO. Explain the implications of not meeting an objective, be clear about what their commitment needs to be, and then get them to commit to it publicly.

They are then as invested in meeting your security objectives as you are. The biggest challenge for many of the CISOs I have worked with is how to communicate and engage with your security team to execute while getting business leaders invested in the process at the same time. As CISO, you need to be able to speak both languages – the business and the technical side of cyber security.

Q. How would you go about prioritizing risk and allocating resources?

This starts with the risk assessment and looking at supplementary information. Look at how many incidents have occurred previously and whether you can isolate where and when they are occurring. Look at things like open positions in the security team, what cyber security training has taken place in the business, what assets the company has (hardware and software), and where the vulnerabilities lie. Only when you have this information can you start prioritizing. Prioritize based on what will support the business objectives best and go from there. Take a holistic view and then allocate resources accordingly.

Q. What tips do you have for creating a culture of security in the business?

It has to come from the top. If your senior leaders are not engaged in your security initiatives, how can you expect the rest of the business to be? The most successful cyber security programs are ones in which the CEO helps to communicate and reinforce their initiatives, ensuring the wider business understands why security is important and the implications of not investing in it. Throughout the year, ensure regular and compulsory company-wide security initiatives, training, and exercises that are occurring and driven by the CEO where appropriate.

Everyone in the business needs to be reminded of their role in supporting a secure environment. Start from the top, be consistent, and make sure everybody plays. Be sure to position security as an enabler of the business rather than a chore within the company. Depending on your industry, security is increasingly becoming a crucial part of the value proposition.

Q. Where do security roadmaps often fall short in your experience?

Security roadmaps usually fall short over asset management. Knowing what assets you have and understanding your data is absolutely vital to creating a security roadmap to protect those assets. I've also seen roadmaps fall short when the CISO has overpromised and then underdelivered in their set timeframe. A roadmap that is too ambitious and then fails to achieve its year-one objectives can result in questioning the security function's effectiveness.

Business leaders often have unrealistic expectations of what can be achieved in a year with available resources. Be realistic about what your team can do within the first year. When creating a multi-year roadmap, create a multi-year budget so that if something is not achieved in the first year, then the budget can be allocated to it in the second year.

Finally, I have seen roadmaps fall short when the CISO is not the one communicating with the board. When other people start representing the cyber security function at the board level, problems can arise. They may not be able to accurately respond to questions or may misquote information, which only leads to confusion and delay. The CISO has to be the one communicating with the board for the long-term success of the security function.

Q. How does the constantly evolving regulatory environment impact the process of creating a security roadmap?

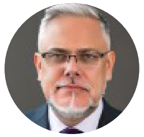
There is a real need for agility to account for the ever-changing regulatory environment. This is the case for businesses across the board as the regulatory environment now impacts every type and size of business, not just what we have previously viewed as highly regulated industries such as finance and insurance. For large companies, the challenge can be managing regulatory changes across multiple territories, while for smaller businesses, it is about achieving compliance with a small budget. Both scenarios are very challenging. Being agile is crucial to managing this.

> “
>
> For a roadmap to be effective, it needs to be understood by business leaders within the organization, whether they have a security background or not.

Jessica Robinson
Founder & CEO
PurePoint International

3 common planning pitfalls for **security leaders**

> “Compliance should happen on the way to security. Compliance shouldn’t be the target. We shouldn’t be in the business of developing security features. We should be in the business of developing features securely.



Mike Wilkes
Security Advisor
Ammolite Analytx, Wallarm & SecurityScorecard

#1 Don’t create security in a silo

Avoid forcing the business to prioritize a technical risk in a certain way without understanding their specific constraints. Accusing the business of developing things insecurely will create bad blood and ultimately diminish collaboration. You’ll always struggle to tell a developer what to do. Your job is to give them the awareness and tools to do their job better.

#2 Don’t be too secretive

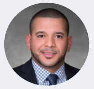
Try to make your roadmap and associated plans 100% public in the organization where possible. Provide full transparency. Articulate to the business what pillar of the plan you are working on at a given moment in time. It allows others to see where security could fit into their roadmap. It will enable you to uncover new partnerships in the organization and help you tie initiatives together.

#3 Don’t be overly compliance-led

Security leaders must immerse themselves in understanding the true risk of compliance rather than preaching on best practice. You can’t afford to become the office of ‘no.’ If the culture is afraid to come to you with a new product or vision, you will only open up more risk to the business. Security needs to be the office of enablement. Compliance is important, but don’t let it lead your program.

Planning advice from **security leaders**

"Create a brand for security. When people see a communication from the office of the CISO and it has that logo, they understand the team it's coming from and what we are here to do. When you create that brand and make yourself available to the user community, they will come to you and have that welcoming approach. It will save you from constantly having to chase the risk."



Brian Lozada - CISO, Prime Video

"You must understand where your risks are coming from. If you have 800 software engineers developing a product, then you have 800 people that could be writing risk every single day. Ask yourself: Have I shifted left? Is security embedded in the CD pipeline? Am I enabling developers to write software in a secure way? Are they even aware of the problem?"

Dan Walsh - CISO, VillageMD

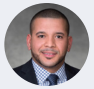
"Bringing in new tools and technology is easy. Changing mindsets is hard. I try to be as radically transparent as possible - partnering with legal, HR, engineering, finance, product, strategy, and marketing to try and figure out where those win-wins are. Looking for opportunities to improve security while allowing the product team to get a bullet point press release out of it."

Mike Wilkes - Security Advisor, Ammolite Analytx, Wallarm & SecurityScorecard

"Create goals for the year based on what you are trying to defend coupled with 6 months of detailed project plans. But ensure you have a 3-month review cycle so that you can track the progress that's been made against the roadmap and determine whether any new priorities have come up. Ignoring new priorities can be a real disservice to your security roadmap."

Sadiq Khan - CISO, BlueVoyant

"At the end of the day, security is there from a support perspective, but it's also there to ensure that customer experience is successful. Security needs to be part of that. So, understanding the business roadmap and aligning your security roadmap accordingly is crucial. This process will also help you identify gaps in your resources."



Brian Lozada - CISO, Prime Video

The cyber security roadmap **checklist**

□ Carry out an external assessment

□ Develop executive support

□ Ensure security objectives align with business goals

□ Assess resource allocation to business as usual activities

□ Build a clear timeline of actions to achieve objectives

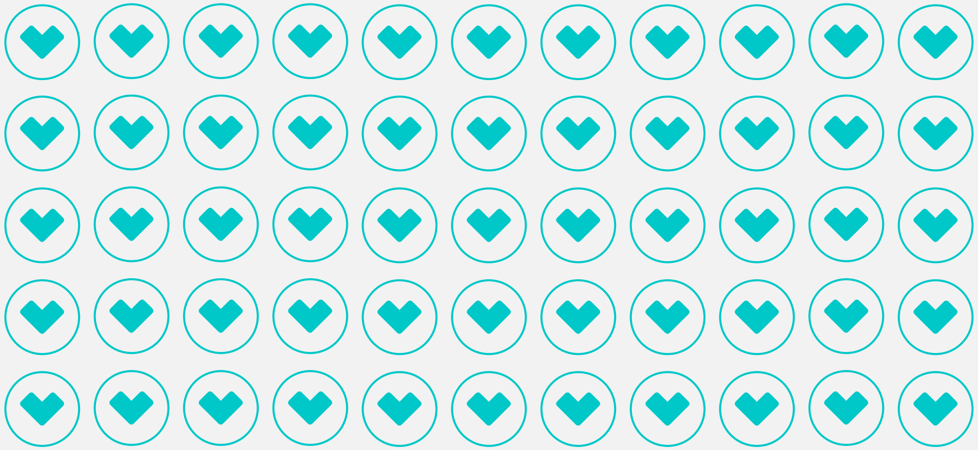
□ Make objectives quantifiable and build scorecard

□ Map out team and partner resources available

□ Hold a contingency fund in your budget for incidents and new priorities

□ Be transparent with your plan and socialise it widely

□ Create a security brand internally



About
Stott and May

Founded in 2009 Stott and May are a professional search firm with a passion for helping leaders achieve complete confidence that they have hired the right talent, first time in fiercely competitive markets. We believe you should never have to make the choice between quality of candidate and time-to-hire. As a result, our business has been founded on the principle of offering a premier standard of search service delivered in vastly accelerated timescales. Because after all this is about more than just recruitment, it's about turning your business vision into reality.

stottandmay.com

STOTTANDMAY