STRIDER

BUILDING AN EFFECTIVE ECONOMIC SECURITY PROGRAM

Three critical components to proactively secure your organization against state-sponsored risk

TABLE OF

CONTENTS

WHAT'S AN ECONOMIC SECURITY PROGRAM?

An economic security program enhances an organization's security and competitiveness by safeguarding its economic interests from state-sponsored actors.

Economic security is a critical component within an organization's overarching security strategy, leveraging data analysis, subject-matter expertise, and various tools to achieve strategic objectives.

Strider's primary goal of an economic security program is to empower decision-makers to make informed choices, anticipate and mitigate potential security challenges, and optimize resource allocation.

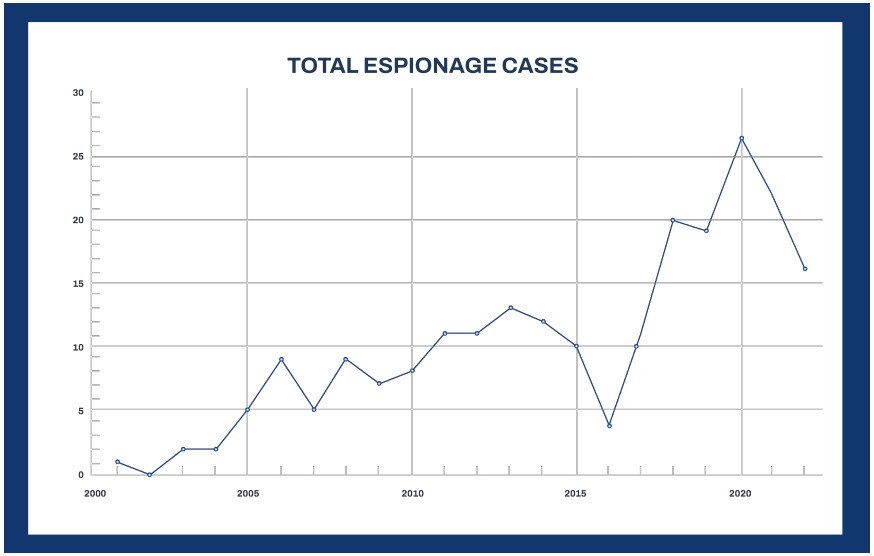
THE STATE OF STATE-SPONSORED RISK

State-sponsored actors are people who engage in malicious activities with the goal of furthering their nation's strategic interests. They often have substantial resources, expertise, and tools at their disposal, making them capable of conducting sophisticated and targeted operations.

Foreign governments and state-sponsored actors have always used tactics to obtain information that could help expand their technological and military prowess. The difference today is how they're going about it.

Historically, state-sponsored actors focused on collecting classified information at a government-to-government level. Today, we also know they focus on growing their strategic advantages through the global economy. They are specifically interested in disruptive technologies such as artificial intelligence (AI), quantum science, semiconductor production, biopharma, and other technical industries. Becoming an industry leader in any of these fields will create a global economic advantage for the nation these actors represent.

In this era of geopolitical competition, many organizations are at a heightened risk of state-sponsored intellectual property theft.



The chart above shows the numbers of publicly reported Chinese espionage incidents over time. Perhaps the most interesting part of this chart is the sharp dip after the 2015 agreement between President Obama and President Xi to restrict commercial espionage by government entities. The decline was quickly reversed within a year of the agreement. [1]

THREE COMPONENTS TO AN EFFECTIVE ECONOMIC SECURITY PROGRAM

All organizations are at different levels of economic security sophistication. Regardless of where your organization is currently, many find success when they embrace an incremental approach. With modest yet targeted initiatives, security teams can progressively craft a robust security program. This structure allows organizations to adapt to evolving threats while fostering a foundation of sustainable protection.

When looking to build up an insider threat program, organizations should focus on three core components: environment, strategy, and education.

1. **Environment:** Teams working exclusively on resolving economic security risk should understand both the external and internal risk environment, especially as it relates to their organization's technology.

2. **Strategy:** Security teams should develop proactive strategies to detect and mitigate related risk.

3. **Education:** Security teams should provide meaningful education to raise employee awareness of state-sponsored risk.

In the upcoming sections, you'll gain insights to evaluate the sophistication level of each of these components within your organization, and you'll discover effective methods for identifying essential next steps for each component.

COMPONENT #1

ENVIRONMENT

Understanding the Internal and External Risk Environment

Awareness is the first step in creating a proactive security response. To effectively secure your organization, you need both an external understanding of what information is being sought by foreign entities and an internal understanding of how state-sponsored actors target your technology and talent.

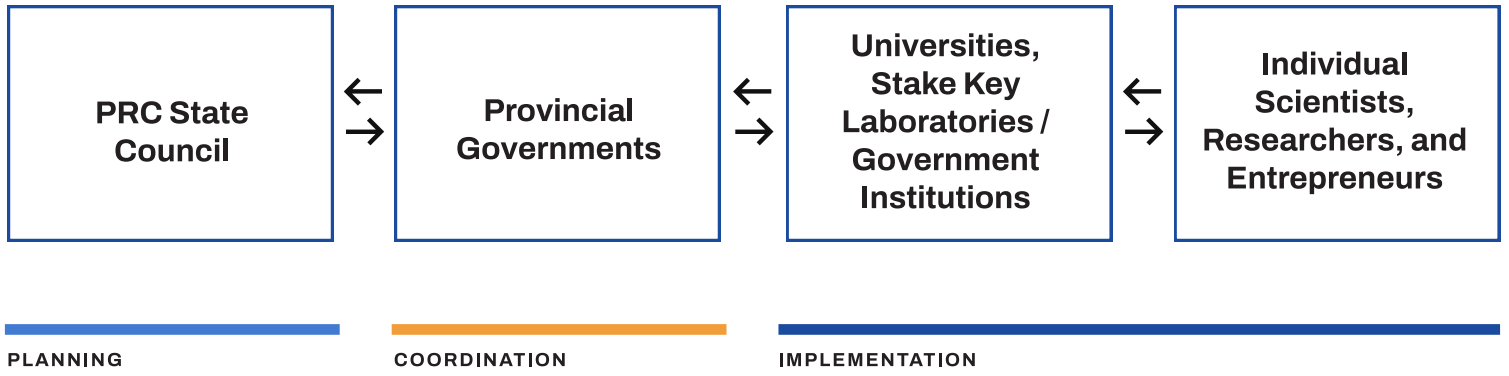
The External Threat Landscape

Foreign governments often employ a systematic approach to obtain desired technology, leveraging economic statecraft and state-sponsored actors. This multifaceted strategy typically involves collaboration between central and local government entities and includes incentive programs designed to advance their technological agendas.

To proactively know which technologies foreign governments are interested in, organizations can review foreign government strategic plans, economic goals, and economic statecraft policies.

Strider's product, Ranger, offers an intuitive dashboard view of this information, and how it overlaps with the innovations at your own company.

The External Threat Landscape with the PRC



The Internal Threat Landscape

One of the biggest challenges for security teams is knowing where to allocate their resources. To do that, first identify the "crown jewels" of the organization—the most critical IP and technologies. Then look at which IP state-sponsored actors have identified for their collection. The overlap of those two areas is where your team should focus their security response.

"The 'Crown Jewels' of an organization are the information or resources that, if stolen or destroyed, would damage, or destroy the enterprise. They are often the materials most sought by outsiders and foreign adversaries. Identifying such crown jewels can help organizations conceptualize the potential for adversaries to target any and all employees who have access to these assets. This common risk management practice can also help focus workforce awareness efforts and help insider threat programs tailor their analysis efforts."

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

In addition to identifying key IP and technologies, understanding how state-sponsored actors work and their recruitment cycle is critical to identify risk in your organization.

Each segment in the cycle provides “breadcrumbs” of relationship building. Being able to spot these segments in your organization helps identify which talent is most likely to be targeted and which talent may already be in communication with bad actors.

Using only open-source intelligence, Strider’s product, Ranger, offers supplemental information on talent that’s at the highest risk of being targeted. This information complements your existing economic security solution and provides crucial context in your investigations.

THE STATE-SPONSORED RECRUITMENT CYCLE

COMPONENT #2

STRATEGY

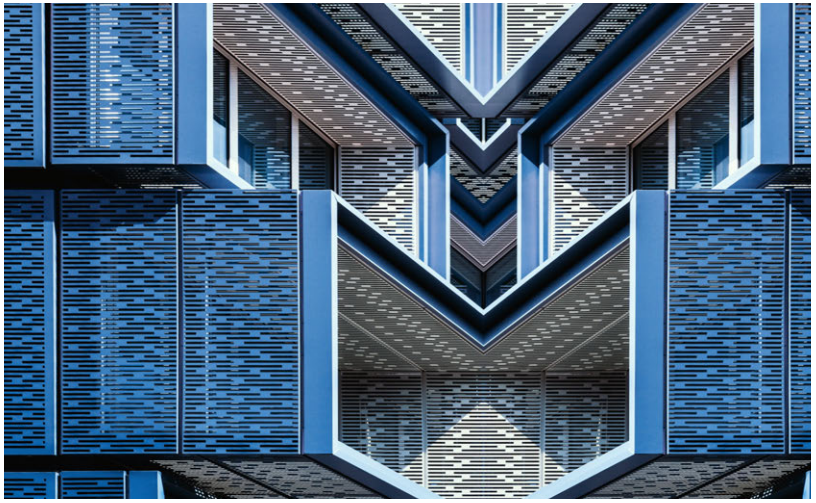
From Reactive to Proactive

With so many potential risks constantly requiring attention, it can be easy to slip into a reactive security response. In this scenario, security teams take an ad hoc approach to incidents, dealing with each one individually as it happens. While this may feel effective due to the amount of work it requires, taking a comprehensive approach and setting up a proactive security posture can create vastly improved results for your organization.

Defendable and Repeatable Processes

Your security team most likely can't protect everything. In the previous section, we covered prioritizing your organization's IP and technology so you can focus your resources on the highest risk to effectively monitor state-sponsored aggression.

With that identified, your team can establish defendable and repeatable processes around keeping that IP and technology secure. Defendable and repeatable processes are crucial components of an effective economic security program. Some of the benefits of having such processes include:



Consistency: Defendable and repeatable processes ensure that the same procedures are followed consistently across different scenarios. This consistency helps reduce the likelihood of errors, omissions, or oversights that might occur when security teams take an ad hoc approach.

Efficiency: With established guidelines and procedures, team members can work more quickly and confidently, reducing the time and effort required to address economic security issues.

Accuracy: Repeatable processes are often accompanied by clear documentation, making it easier to track and verify the steps taken. This documentation reduces the risk of errors or misunderstandings that could exacerbate economic vulnerabilities.

Putting a proactive security response in place involves several key steps, including identifying the process scope and purpose, documenting process steps, defining roles and responsibilities, establishing decision criteria, and gathering the relevant stakeholders.

COMPONENT #3

EDUCATION

Communication Builds Trust

Educating your people, stakeholders, and executives in a thoughtful way empowers them to make wise decisions to avoid getting entangled in relationships which could hurt them and the company.

Most of all, performing routine training increases the environment of trust in your organization. A workplace with high levels of trust is not only a more desirable place to work, it also leads to higher levels of risk reporting and ultimately better protected IP.

Targeted Trainings

Identify which of your employees has access to critical technologies and IP that state-sponsored actors are after. Conduct special security training with these individuals and be clear that they are a target. Preemptively teaching them the tactics, techniques, and procedures of state-sponsored actors will empower them to recognize the signs when approached.

Employee Trainings

Security is everyone's responsibility. Ensure that all employees in the company know what to look out for and how to react to potential risks. Transparent education builds an atmosphere of trust throughout the entire organization.

Executive Briefings

Executive buy-in is critical for a robust security program. Conducting regular briefings helps align your stakeholders' understanding of state-sponsored risk, company risk tolerance, cultures of trust, and related messaging. It's the role of the economic security team to educate and emphasize the importance of having an effective economic security program.

Post-Training Analysis

Best practices recommend conducting a follow-up meeting and/or survey after all briefings and training to measure their effectiveness. Are employees generally more aware of potential risks? Create a strategy to measure the results of each briefing and training.

Channels for Sharing Concerns

Put a reporting system in place if you haven't already done so. Always encourage them to err on the side of reporting. State-sponsored theft attempts should be a known and talked about concept with employees.

WHY SPY?

The paper titled “Why Spy?: The Psychology of Espionage” by Dr. Ursula M. Wilder found that all espionage cases have three common factors:

1. **Dysfunctional personality**—an ego that can justify violating trust

2. **State of crisis**—there is a perceived need to take the risk

3. **Ease of opportunity**—they believe they can get away with the act

Considering these factors can help navigate internal investigations.

IP Theft occurs at the intersection of opportunity, crisis, and personality.

UPGRADE YOUR SECURITY PROGRAM WITH OPEN-SOURCE INTELLIGENCE

Strider is an AI-powered intelligence firm specializing in risk management and business competitiveness. Using only open-source data, we provide critical context and insights that can benefit security teams, talent acquisition teams, supply chain risk management teams, and more.

OUR SUITE OF PRODUCTS

Ranger

Ranger helps identify, visualize, and respond to state-sponsored risks within your organization. Utilizing our proprietary open-source methodology, Ranger helps identify technology and talent that are at the highest risk of being targeted by state-sponsored actors.

Checkpoint

Checkpoint enables organizations to thoroughly screen potential third-party partners for any connections to sanctioned or restricted entities and subsidiaries, including state-owned organizations.

Shield

Shield is our premiere email security product. It enables security teams to block, monitor, and investigate inbound emails originating from sanctioned, restricted, or state-owned entities.

Sentry

Sentry empowers organizations to safely meet their talent needs by illuminating an individual's potential connections to state-sponsored risk, including talent, partners, and collaborators.

SERVICES

In addition to our suite of intelligence products, we offer tailored, hands-on security development. Services is designed to elevate and transform nascent and developing economic security initiatives into mature and advanced programs.

No matter the level of your organization's program sophistication, move from a reactive to a proactive security protocol based on comprehensive analysis and insights.

CASE STUDY

AN EFFECTIVE ECONOMIC SECURITY PROGRAM IN ACTION

Overview

Strider's client is a Fortune 100 technology company that operates in a highly competitive and innovative industry. With a wide range of cutting-edge technologies and a significant talent pool, our client recognizes the need to protect their intellectual property (IP), technology, talent, and supply chain from state-sponsored risks. To achieve this objective, the organization leverages Strider's suite of products, particularly Ranger, to proactively identify potential risks and safeguard their critical assets.

Proactive Over Reactive

Facing the constant risk of state-sponsored actors targeting their technologies and talent, our client sought to establish a proactive security response. The security team began by strategically safeguarding their most vulnerable areas first. For their organization, that meant identifying the technologies actively pursued by state-sponsored actors and securing employees with expertise in those areas.

To identify these areas, the client utilized Strider's Ranger. Thanks to the open-source intelligence of Strider's products, the security team immediately gained critical insights into most-sought technologies and identified employees with valuable expertise who were likely to be approached by state-sponsored actors for their knowledge.

Collaborating closely with Strider's Intelligence Team and security subject-matter experts, the client then designed and executed a proactive security strategy. They provided targeted employees with comprehensive training, equipping them with the knowledge to detect the common tactics, techniques, and procedures (TTPs) employed by state-sponsored actors. They ensured that the employees were well prepared to respond effectively should they ever face an approach from state-sponsored actors.

Spotting a Recruitment Attempt

Just two weeks after the proactive defense training, one of the employees received a message via LinkedIn from a state-sponsored actor, promising a substantial amount of money and additional benefits to work for an overseas company. The employee recognized the approach as a targeted state-sponsored threat and promptly reported the incident to the security team.

In response to the message, the client continued collaborating with Strider to gather more information about the sender. Strider's investigation revealed that the individual belonged to a company directly backed by a foreign government, with the intention to compete directly with the client.

This incident demonstrated the effectiveness and timeliness of the client's proactive security strategy. By leveraging Strider's Ranger and carefully and proactively equipping their employees with the necessary knowledge and tools, the client successfully safeguarded a critical talent of the company.

As state-sponsored risk continues to increase and pose a threat to both the public and private sector, developing an economic security program can be your best defense.

Regardless of your program sophistication, getting a better understanding of your risk environment, transitioning to a proactive security protocol, and implementing proper education and training are critical for your team's success and organization's security.

Reach out to a Strider representative today to learn how Strider can better assist your program development.

STRIDERINTEL.COM