How to build a top-class cybersecurity team and when to outsource

BY ANNA HAMMOND · JUNE 27, 2024 · LAST UPDATED ON NOVEMBER 13, 2025

Ask any cybersecurity leader what keeps them awake at night, and they'll likely tell you it's the thought of falling victim to a cyberattack. Indeed, cyberattacks are a significant concern for most leaders, with the potential to compromise data, disrupt operations, and cause substantial reputational and financial damage. While it's true that people can be your biggest security risk, they can also be your greatest asset. That's precisely why building a robust cybersecurity team is so essential.

However, assembling such a team team comes with challenges, particularly in talent acquisition and management. Moreover, the cybersecurity field faces a significant talent shortage, with demand for skilled professionals exceeding supply.

Consequently, many organizations now look to outsourcing as a practical solution, gaining access to specialized skills and up-to-date knowledge that might be too costly or difficult to develop in-house. It also offers flexibility and scalability, allowing organizations to adjust their cybersecurity capabilities in response to changing threats and business needs.

Whether by developing internal expertise or utilizing external resources, the strategies outlined in this guide will offer valuable insights into establishing a resilient and effective cybersecurity function.

Understanding Cybersecurity Team Structures

A cybersecurity team structure refers to the organized framework of roles and responsibilities designed to:

- Protect an organization's digital assets
- Ensure compliance with regulations
- Respond to security incidents
- Maintain a proactive stance against potential threats.

This structure is crucial as it dictates the efficiency and effectiveness with which cybersecurity challenges are addressed, directly impacting the organization's ability to safeguard sensitive information and maintain operational integrity.

The primary objectives of a cybersecurity team include the protection of assets, ensuring compliance with legal and regulatory requirements, adeptly responding to security incidents, and fostering a security-first culture that anticipates and mitigates risks. To achieve these goals, the team must be well-rounded, with capabilities ranging from technical expertise to strategic risk management.

Conducting a SWOT Analysis Before Building Your Team

When preparing to build or enhance a cybersecurity team, organizations can benefit from conducting a thorough preparatory analysis such as a **SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis**. This strategic planning technique helps identify not only the internal capabilities and challenges of the organization's current security posture but also external opportunities and threats.

Such an analysis informs hiring decisions by clarifying which skills and qualities are necessary in team members to address existing gaps and leverage potential growth areas.

Ultimately, the structure of a cybersecurity team should be dynamic, capable of evolving in response to new security technologies and shifting threat landscapes. By grounding the team's formation in strategic analysis and clear objectives, organizations can ensure a robust defense against the myriad of cyber threats they face today. This strategic approach not only helps in immediate threat mitigation but also supports long-term resilience and security compliance.

Securing buy-in and budget for a cybersecurity team

Organizations can benefit from a wide variety of technologies and tools to safeguard digital assets, but without the right people in place, you'll only skim the surface. Securing buy-in and budget for a cybersecurity team, therefore, is critical.

The process involves not only demonstrating the potential financial and reputational risks of inadequate security measures but also highlighting the strategic value that a robust cybersecurity framework adds to the business.

Why security buy-in matters

To secure security buy-in you'll want to start by ensuring your cybersecurity efforts align with the organization's business strategy. Without that integration, securing the necessary budget for cybersecurity initiatives can be challenging.

Buy-in also facilitates smoother coordination across different departments, enhancing the overall effectiveness of the cybersecurity measures implemented.

While considering the potential return on investment (ROI) is important in certain scenarios, emphasizing Return on Prevention (ROP) offers a clearer illustration of the benefits of having robust cybersecurity infrastructures. It also highlights the significant risks associated with the *absence* of such protections.

Cybersecurity leaders must articulate the direct and indirect costs associated with data breaches, including downtime, legal fees, loss of customer trust, and potential fines for non-compliance with regulations.

Budgeting for cybersecurity success

Once you secure buy-in, the next step is budgeting. As previously mentioned, framing cybersecurity as an investment in prevention rather than a cost can have a more significant impact. Allocate funds based on risk assessments and business priorities. Budgets should cover:

- Essential tools and technologies
- Hiring talent
- Training staff
- Planning for incident response
- Conducting regular audits and assessments.

It's crucial for organizations to be realistic about their cybersecurity needs and to prioritize spending on areas that will provide the greatest impact in terms of risk reduction.

Cost-Efficient Alternatives to In-House Hiring

For many organizations, even medium-sized to large enterprises, the high cost of building and maintaining an extensive in-house cybersecurity team can be prohibitive. Similarly, it's unrealistic to expect employees to stay expertly informed about the rapidly changing threat landscape. Combining internal and external expertise can significantly strengthen your cybersecurity setup without overextending your team.

Organizations can consider forms of partnership and collaboration to enhance their cybersecurity capabilities. This might include outsourcing certain security functions to specialized firms, collaborating with other companies for shared security services, or participating in industry-wide security initiatives.

Key roles in a cybersecurity team

Each role within a cybersecurity team is like a piece in a complex puzzle. From strategic oversight to technical defense and compliance enforcement, these roles collectively ensure a robust defense mechanism is in place to counteract rapidly evolving cybersecurity challenges. Here's a closer look at some of the key roles that are fundamental in maintaining an organization's cybersecurity posture, along with insights on when it's best to hire internally or externally.

Chief Information Security Officer (CISO) – internal resource

The CISO is a senior-level executive responsible for developing and implementing the security strategy of an organization. This role involves overseeing the security program, aligning security initiatives with business objectives, and ensuring that the organization's digital assets and technologies are protected against potential threats. The CISO also plays a crucial role in risk management and is often involved in policy development, staff training, and crisis management.

Security analysts – internal resource

Security analysts are on the front lines of cybersecurity operations. Their primary responsibilities include monitoring security systems for anomalies and signs of breaches, analyzing security threats, and responding to security incidents. They use a variety of tools to detect and mitigate threats and are pivotal in maintaining the integrity and confidentiality of company data.

Security engineers – internal resource

These professionals are tasked with the design, implementation, and maintenance of security solutions that protect organizations from potential threats. Security engineers work closely with other IT professionals to ensure that the security infrastructure is integrated seamlessly with other systems. Their work includes installing firewalls, configuring anti-virus systems, and securing network infrastructures.

Penetration testers (ethical hackers) – external resource

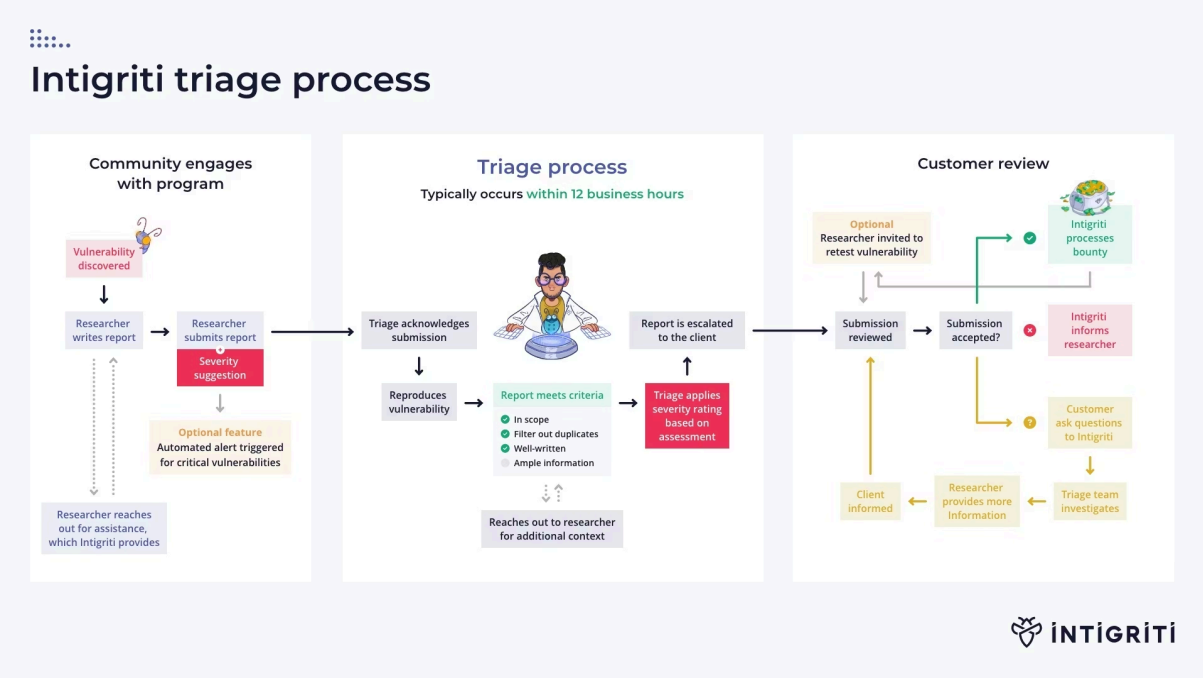
Penetration testers, or ethical hackers, play a unique role by actively attempting to breach computer systems, networks, and applications using the same techniques as potential attackers. Their goal is to identify and fix vulnerabilities before malicious hackers can exploit them. This proactive approach is critical in fortifying security defenses.

While many companies employ full-time pentesters, others prefer to engage external partners to gain an outside perspective. In recent years, bug bounty platforms have emerged as a solution to extending the ethical hacking capabilities of in-house cybersecurity teams.

They offer a cost-efficient way to test security without a huge investment in internal resources because they allow organizations to leverage the skills and knowledge of thousands of security researchers who test the organization's systems for vulnerabilities.

This approach means companies benefit from a diverse range of perspectives and expertise, which can lead to the discovery of security flaws that might otherwise go unnoticed.

Bug bounty programs are typically based on a pay-for-results model, meaning organizations only pay when a vulnerability is identified. This can be more cost-effective compared to the ongoing costs associated with full-time security staff. Additionally, these programs can reduce some of the administrative and manual tasks of managing vulnerabilities that burden over-stretched security teams. As a result, your team can more clearly focus on strategizing and improving overall security posture. A good example of this in action is the triaging process, as outlined below.



Incident response team – internal resource

This team is critical when a security breach occurs. Members of the incident response team are trained to manage and mitigate security incidents efficiently. Their responsibilities include conducting a thorough investigation to understand the scope and impact of the breach, containing the breach to prevent further damage, and leading recovery efforts to restore systems and operations.

Compliance officers – internal or external resource

Compliance officers ensure that an organization adheres to external regulatory requirements and internal policies. In the context of cybersecurity, they are responsible for ensuring that the organization complies with laws and regulations related to data security and privacy. This role involves regular audits, compliance checks, and coordinating with legal teams to keep up to date with the latest requirements.

Security architects – internal resource

Security architects are responsible for designing the blueprint of an organization's security systems. Their role involves creating a robust security architecture that aligns with the organization's business goals and technology infrastructure. They assess current security measures and propose enhancements, ensuring that all security solutions are integrated and operate effectively to protect against threats.

Together, these roles form a comprehensive cybersecurity team that is essential for protecting an organization's information assets against the increasing threat of cyberattacks. Each role complements the others, ensuring a well-rounded approach to cybersecurity management.

Building a robust cybersecurity team

Building a robust cybersecurity team involves several key steps, from defining team goals to fostering a collaborative culture. Here's how you can build a top-class cybersecurity team that not only defends against immediate threats but also prepares for future challenges.

Defining team goals and objectives

The first step in building a cybersecurity team is to establish clear, measurable goals and objectives. This clarity helps in aligning the team's efforts with the organization's overall security strategy. For example, setting a goal to reduce the average time to detect and respond to incidents can drive improvements in processes and technology, such as vulnerability reporting, enhancing the team's efficiency and effectiveness.

Goals should be specific, measurable, achievable, relevant, and time-bound (SMART) to ensure they are practical and actionable.

Recruiting the right talent

Attracting and hiring skilled cybersecurity professionals is perhaps the most challenging aspect of building a cybersecurity team. The demand for experienced cybersecurity talent often outstrips supply. To address this, organizations can partner with cybersecurity staffing agencies that specialize in this field. Additionally, attending industry conferences and networking events can help in meeting potential candidates and promoting your organization as an employer of choice. Offering competitive salaries, benefits, and opportunities for career advancement can also attract top talent.

Providing ongoing training and development

A recent poll by Intigriti found that around half (49%) of security professionals find a lack of time the biggest challenge for keeping up with threats. Other challenges included:

- The volume and diversity of threats: 40%
- Staying up to date with the latest security testing tools and techniques: 34%
- Limited resources for training: 31%
- Sophistication of cyber-attacks: 29%
- Lack of visibility into emerging threats relevant to organizations: 20%

Cyber threats continually evolve, and so must the skills of your cybersecurity team. Investing in ongoing training and professional development is essential. For example, supporting team members to pursue and maintain industry-recognized certifications such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), or Certified Information Security Manager (CISM) can enhance their skills and knowledge.

For continuous development, launching a bug bounty program can provide a practical, ongoing learning environment that sharpens a team's cybersecurity capabilities. By engaging with ethical hackers who use diverse, innovative techniques, teams gain exposure to real-world vulnerabilities beyond typical training scenarios.

This continuous interaction keeps the team updated on the latest cybersecurity trends and challenges. Analyzing external hackers' approaches helps internal teams benchmark and enhance their skills, fostering better problem-solving and defensive strategies.

Additionally, the collaborative nature of addressing these vulnerabilities improves teamwork and communication within the team.

Fostering a collaborative culture

Cybersecurity is not a one-person job; it requires a coordinated effort across different roles and departments. Promoting a culture of teamwork and open communication is vital. Regular team meetings and collaborative projects can help in building trust and ensuring all team members are on the same page. Cross-functional collaboration with IT, legal, and compliance teams can also provide broader perspectives and enhance the cybersecurity team's effectiveness. Creating a supportive environment where team members can learn from each other and share knowledge freely contributes significantly to the team's success.

Implementing a clear reporting structure

A clear reporting structure is critical to the smooth operation of the cybersecurity team. It ensures that information flows efficiently from the front lines to top management. For instance, security analysts might report to security managers, who then report to the Chief Information Security Officer (CISO). This hierarchy helps in maintaining order, ensuring accountability, and facilitating quick decision-making in response to security incidents. It also clarifies roles and responsibilities, which is essential for operational efficiency.

Best practices for managing a cybersecurity team

To ensure that the team is efficient, motivated, and up to date with the latest cybersecurity techniques, here are some best practices for managing a cybersecurity team:

Regular performance reviews

Regular performance reviews are essential for assessing the effectiveness of team members and providing constructive feedback. Implementing quarterly performance reviews can be particularly effective. During these sessions, managers should evaluate each team member's contributions and challenges, discussing any areas for improvement.

It's also beneficial to develop personalized development plans during these reviews, which can help guide team members in their career growth and skill enhancement. This not only helps in keeping the team's skills sharp but also boosts morale by showing team members that the organization is invested in their personal and professional development.

Staying current with industry trends

The cybersecurity landscape is constantly changing, with new threats and technologies emerging regularly. It's vital for cybersecurity teams to stay informed about these developments. Managers can facilitate this by:

- Subscribing to reputable cybersecurity news feeds

- Encouraging team members to attend industry webinars
- Launching bug bounty programs
- Providing opportunities for professional development through courses and certifications.

This continuous learning environment helps the team anticipate and react to new threats more effectively, ensuring the organization's defenses remain robust.

Encouraging innovation

Cybersecurity challenges require innovative solutions, and fostering an environment that encourages creativity is key. One way to promote innovation within a cybersecurity team is by hosting hackathons and internal competitions. These events can motivate team members to think outside the box and develop unique solutions to complex security problems. Additionally, these activities can serve as team-building exercises, enhancing collaboration and communication among team members.

Establishing incident response protocols

Having a well-defined incident response protocol is critical for minimizing the impact of security breaches. This involves creating and maintaining comprehensive incident response plans that outline specific procedures for various types of security incidents.

Regularly updating and testing these procedures is crucial to ensure they remain effective under different scenarios. Conducting drills and simulation exercises can help the team practice their response to a security incident, making them better prepared for real-life situations.

Tools and technologies for cybersecurity teams

Cybersecurity teams rely on a variety of tools and technologies to protect digital assets, detect threats, and respond to incidents. Among the most critical tools are Security Information and Event Management (SIEM) systems, Endpoint Detection and Response (EDR) solutions, and firewalls.

Automation can lead to significant efficiency gains for cybersecurity teams by reducing the manual workload of security analysts by automating repetitive tasks such as log analysis, alert generation, and incident response actions. This not only speeds up response times but also allows cybersecurity professionals to focus on more complex and strategic activities.

Integration of cybersecurity tools is equally important. For instance, integrating SIEM with EDR and threat intelligence platforms can provide a more comprehensive view of the security landscape and improve the detection of sophisticated threats. This holistic approach enables faster and more accurate threat detection and response by allowing different tools to work together seamlessly.

Customization and scalability

Each organization has unique security needs based on its industry, size, and specific risk factors. Therefore, customizing cybersecurity tools to fit these needs is crucial. Customization can involve setting specific security policies, tuning the sensitivity of anomaly detection systems, or creating customized dashboards for better visibility.

Scalability is another critical consideration. As organizations grow, their cybersecurity tools must be able to scale accordingly. This means that tools should be capable of handling increased loads, more endpoints, and larger volumes of data without compromising performance. Scalability ensures that the security measures grow in tandem with the organization, providing continuous protection regardless of size.

Knowing when to outsource cybersecurity

Building a top-class cybersecurity team requires a strategic approach to defining goals, recruiting talent, training, fostering collaboration, and establishing a clear organizational structure. By focusing on these areas, organizations can develop a capable and responsive cybersecurity team that not only addresses current security needs but also adapts to future challenges, ensuring long-term protection and resilience.

However, it's important to weigh up the benefit of hiring in-house or outsourcing skills to external experts. Doing so means organizations can benefit from the latest techniques and tools in cybersecurity, ensuring thorough testing and validation of their security measures without the need for long-term investment in specialized personnel.

Conclusion: Strengthening Your Security with Intigriti

Intigriti is the trusted leader in crowdsourced security. Since 2016, we've empowered the world's largest organizations, such as Coca-Cola, Microsoft, and Intel, to proactively identify and address vulnerabilities before they're exploited by cybercriminals. Our dynamic pool of 125,000+ researchers help businesses to promptly detect vulnerabilities and avoid damaging security breaches. To find out how our community, as well as our customer success and triaging experts, can become an invaluable extension of your team, contact us today.