NCDIT 2022 Cybersecurity Summit

Grow Your Own SecOps Team

Presented by

Isabelle Hertanto
About Info-Tech Research Group

Info-Tech Research Group produces unbiased and highly relevant research to help leaders make strategic, timely, and well-informed decisions. We partner closely with your teams to provide everything they need, from actionable tools to analyst guidance, ensuring they deliver measurable results for the organization.

Drive Measurable Results
Our world-class leadership team is continually focused on building disruptive research and products that drive measurable results and save money.

Better Research Than Anyone
Our team of experts is composed of the optimal mix of former CIOs, CISOs, PMOs, and other IT leaders and IT and management consultants, as well as academic researchers and statisticians.

Leverage Industry Best Practices
We enable over 30,000 members to share their insights and best practices that you can use by having direct access to over 100 analysts as an extension of your team.
Who am I?

- Background in Software Development
- Former Canadian Spy - turned Corporate Risk Manager - turned Cybersecurity Consultant
- Teacher
- Dog Mom
What kind of Cybersecurity professional are you looking for?
Looking for a Senior Cybersecurity Analyst

- University degree in IT, information security, or related field
- 10-15 years of experience
- CISSP and CISM or equivalent
- MBA an asset
- Must wear multiple hats
- Asking salary must be between $100-140K
Looking for a Senior Cybersecurity Analyst

Cybersecurity Unicorn

• University degree in IT, information security or related field
• 10-15 years of experience
• CISSP, CISM or equivalent
• MBA an asset
• Must wear multiple hats
• Asking salary must be between $100-140K
REMINDER: Unicorns aren’t real.
IT leaders must do more to attract talent

3.5 million unfilled cybersecurity openings in 2021

Source: Cybercrime Magazine, 2021
IT leaders must do more to attract talent

US$185,500 is what top earners make annually across the United States.

Source: ZipRecruiter
30% of the current cybersecurity workforce plans to change professions.

2022 Trellix survey: A Closer Look at the Cyber Talent Gap
IT leaders must do more to retain talent

According to the 2022 Trellix survey: A Closer Look at the Cyber Talent Gap, the top frustrations in the field are as follows:

- Limited support for skills development: 36%
- Lack of recognition: 36%
- Limited support with qualifications/certifications: 32%
- Unclear career progression routes: 27%

Info-Tech Research Group
Growing your own security team

Adopt a people-first approach to resourcing that emphasizes the development and retention of existing staff.

1. OUTSOURCE WITH CARE
2. OPTIMIZE WORKFLOWS
3. FOSTER LEADERSHIP
4. HIRE NEW GRADS
5. TRAIN YOUR PEOPLE
1. Outsource with Care
Outsourcing provides access to tools and talent that would otherwise be prohibitively expensive. Typical reasons for outsourcing security operations include:

- Difficulty finding or retaining security staff with advanced and often highly specialized skillsets.
- The desire to transfer liability for high-risk operational activities such as 24/7 security monitoring.
- Workforce scalability to accommodate irregular or infrequent events such as incident response and incident-related forensic investigations.

Given the above, three different models have emerged for the operational security organization:

1. **Outsourced SecOps**
   - A fully outsourced Security Operations Center, managed and governed by a smaller in-house team

2. **Balanced Hybrid**
   - In-house operational security staff with some reliance on managed services

3. **In-House SecOps**
   - A predominantly in-house security team, augmented by a small managed services contract

Use Info-Tech's blueprint [Develop Your Security Outsourcing Strategy](#) to determine the right approach for your business needs.
2. Optimize Workflows
Top Three CIO Pain Points

1. Staff sufficiency, skill, and engagement issues
2. Business frustration with IT’s failure to deliver value
3. IT limitations that affect business innovation and agility

Source: Info-Tech’s CEO-CIO Alignment Program, 2021; N=446

The Solution

As industries evolve and adopt more tools and technology, their IT operating models become more complex. Process optimization and automation are needed to simplify complex operations and align processes with organizational goals.
Optimize your Security Operations Workflow

Automation: There is a shortfall in human capital in contrast to the required tools and processes. Automate the more trivial processes. Cross-train employees throughout different silos. Enable them to wear multiple hats.

Dashboards: Centralized visibility, threat analytics, and orchestration enables faster threat detection with fewer resources.

Practice: None of the processes happen in vacuum. Make the most of tabletop exercises and other training exercises.

SOCs with 900 employees are just as efficient as those with 35-40. There is an evident tipping point in marginal value.

Adding more controls to a network never increases resiliency. Identify technological overlaps and eliminate unnecessary costs.

There are no plug and play technological solutions – each is accompanied by a growing pain and an affiliated human capital cost.

Define appropriate use cases and explicitly state threat escalation protocol. Focus on automating the tier 1 analyst role.

Planning: Narrow the scope of operations to focus on protecting assets of value.
Consider the following when adopting new tools...

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Will staffing levels change? Will job titles or roles change for certain individuals?</td>
<td>- How will knowledge sharing be enabled so that all analysts can quickly access known errors and resolve problems?</td>
<td>- Is an existing tool extensible?</td>
</tr>
<tr>
<td>- How will staff be reorganized?</td>
<td>- How will procedures be documented so that processes are escalated properly?</td>
<td>- If so, can it integrate with essential non-IT systems?</td>
</tr>
<tr>
<td>- Will staff need to be relocated to one location?</td>
<td>- Will ticket classification and prioritization schemes need to change?</td>
<td>- Can the tool support a wider user base?</td>
</tr>
<tr>
<td>- Will reporting relationships change? How will this be managed?</td>
<td>- Ticket input (i.e. how can tickets be submitted?)</td>
<td>- Can the tool support all areas, departments, and technologies it will need to after consolidation?</td>
</tr>
<tr>
<td>- How will performance measurements be consolidated across teams and departments to focus on the business goals?</td>
<td>- Ticket resolution (i.e. how will resolution be defined and how will users be notified?)</td>
<td>- How will data from existing tools be migrated to the new tool?</td>
</tr>
<tr>
<td>- Will there be a change to career paths?</td>
<td>- Communication with end users (i.e. how and how often will stakeholders be notified about the status of tickets or of other incidents/outages?)</td>
<td>- What implementation or configuration needs and costs must be considered?</td>
</tr>
<tr>
<td>- What will consolidation do to morale, job interest, job opportunities?</td>
<td></td>
<td>- What training will be required for the tool?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- What other new tools and technologies will be required to support the optimized state of security operations?</td>
</tr>
</tbody>
</table>
3. Foster Leadership
The days are gone when the security leader can stay at a desk and watch the perimeter. The rapidly increasing sophistication of technology, and of attackers, has changed the landscape so that a successful information security program must be elastic and nimble, and must be tailored to the organization’s specific needs.

The CISO is tasked with leading this modern security program, and this individual must truly be a Chief Officer, who has a finger on the pulses of the business and security processes at the same time. The modern, strategic CISO must be a master-of-all-trades.

A world-class CISO is a business enabler who finds creative ways for the business to take on innovative processes that provide a competitive advantage, and most importantly: to do so securely.

Cameron Smith
Research Lead, Security & Risk Practice
Info-Tech Research Group
Through these three over-arching behaviors, the CISO can enable a security culture and program that is elastic, flexible, and nimble enough to maintain business process alignment.

Three key behaviors of a world-class CISO

- Aligning security with business requirements
- Enabling a culture of risk management
- Managing talent and change
8 Core Competencies to support the CISO

- Business Acumen
- Leadership
- Communication
- Technical Knowledge
- Innovative Problem Solving
- Vendor Management
- Change Management
- Collaboration

Use Info-Tech's blueprint *Hire or Develop a World-Class CISO* to find a strategic and security-focused champion for your organization.
4. Hire New Grads
People may not be aware of the breadth of apprenticeship programs in the Federal government... We think apprenticeships could be a very exciting way to bring in talent."

Marian Merritt, deputy director of the National Initiative for Cybersecurity Education (NICE)-NIST
State Apprenticeship Data FY 21

North Carolina
Active Apprentices: 8,775
New Apprentices: 608
Completers: 520
Active Programs: 1,055
New Programs: 128

Professional, Scientific, and Technical Services: 1,897

Source: U.S. Department of Labor
5. Train Your People
According to a recent Microsoft Study, 76% of employees say they would stay at their company longer if they could benefit more from learning and development support.

Source: Tech.co
Info-Tech Learning Assurance Framework

Learn Key Concepts and Best Practices

- Interactive Classrooms
- Collaboration Sessions
- Discovery Exercises
- Case Studies

Direct Development Through Targeted Assessments

- Formative Assessments
- Summative Assessments
- Final Assessment

Get Hands-On Experience While Creating Deliverables for the Organization

- Deploy Cyber Range
- Run Practical Exercises
- Create Operational Deliverables
So, where do we start?
Start by upskilling your IT staff!

Turn your IT staff into security professionals by providing them with the necessary security skills to succeed in their area of expertise.

IT Systems Administrator

IT Systems Administrator + Security Skills

IT Security Systems Administrator

Image: ©2018 The LEGO Group. All Rights Reserved.
Discussion and Q & A
Thank You!

For more information please contact:

ihertanto@infotech.com

www.linkedin.com/in/isabelle-hertanto