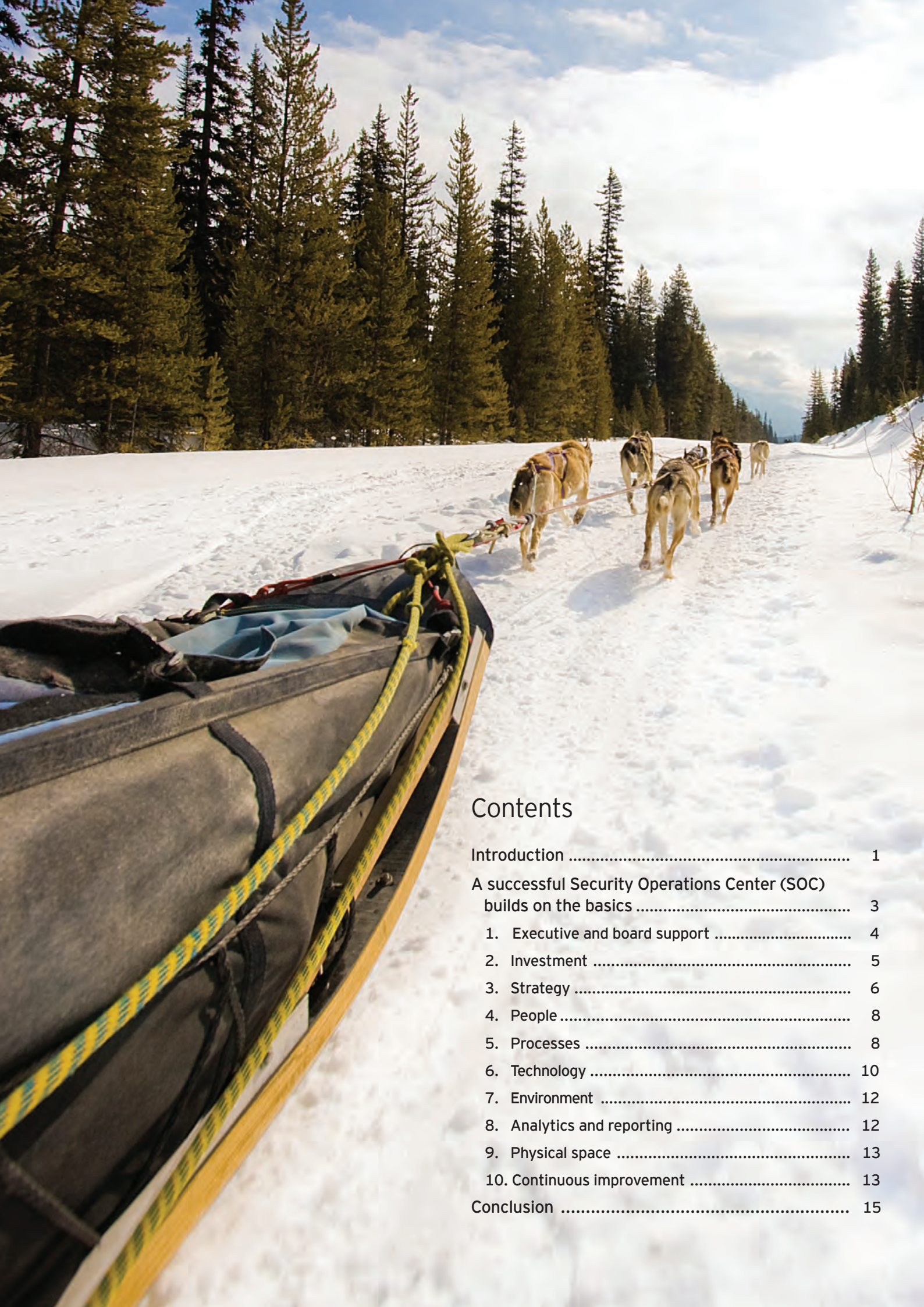
Insights on
governance, risk
and compliance

October 2014

Security Operations Centers – helping you get ahead of cybercrime

EY

Building a better
working world



Contents

Responding faster to cyber threats

Information security is changing at a rapidly accelerating rate. Hackers are increasingly relentless, making the response to information security incidents an ever more complex challenge. According to *EY's Global Information Security Survey 2014*, 67% of respondents have seen an increase in external threats in the last 12 months.*

In today's world of "always-on" technology and insufficient security awareness on the part of users, cyber attacks are no longer a matter of "if" but "when." We live in an age where information security prevention is not an option.

Point solutions (antivirus, IDS, IPS, patching and encryption, etc.) remain a key control for combatting today's known attacks; however, they become less effective over time as hackers find new ways to circumvent controls.

Preparing for known attacks is hard enough. But how do organizations build controls for the security risks they don't even know about yet?

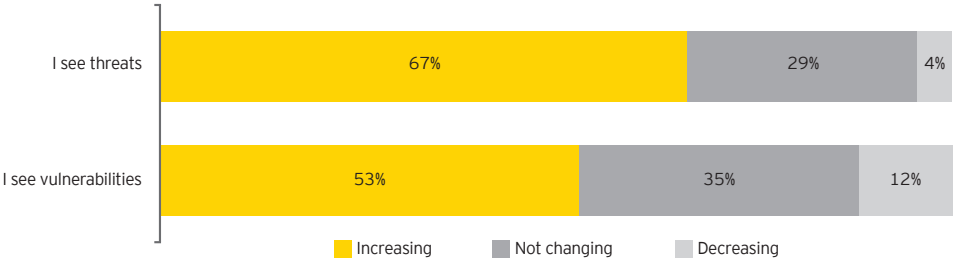
Leading organizations are doing more than improving on their current state. They are seeking to expand their efforts – take bolder steps – to combat cyber threats. Rather than waiting for the threats to come to them, these organizations are prioritizing efforts that enhance visibility and enable a proactive response through monitoring, analytics and prompt detection. Organizations may not be able to control when information security incidents occur, but they can control how they respond to them. Expanding detection capabilities is the key place to start.

A well-functioning Security Operations Center (SOC) can form the heart of effective detection. It can enable information security functions to respond faster, work more collaboratively and share knowledge more effectively. In the pages that follow, we explore the top 10 areas organizations need to consider to make their SOC a success.

56%

of respondents say that it is "unlikely or highly unlikely" that their organization would be able to detect a sophisticated attack.

How has the information security risk environment in which you operate changed in the last 12 months?*



*All survey statistics in this report refer to EY's 17th Global Information Security Survey 2014 which captures the responses of 1,825 C-suite leaders and Information Security and IT executives/managers, representing most of the world's largest and most-recognized global companies. Responses were received from 60 countries and across nearly all industries. For further information, please access: www.ey.com/GISS2014.

Cyber attacks are no longer a matter of "if," but a matter of "when."

With the understanding that attacks can never be fully prevented, companies should advance their detection capabilities so they can respond appropriately.

A successful SOC builds on the basics

Start with the basics. It seems obvious enough. And yet, it's where organizations struggle the most.

Forget the fancy tools and flashy rooms with large screens and biometric scanners in the entryway. They aren't the silver bullet that will protect you from the cyber threats outside – or already inside – your security perimeter.

At the core of a successful SOC is a strong foundation for operational excellence driven by well-designed and executed processes, strong governance, capable individuals and a constant drive for continuous improvement to stay ahead of the cyber adversaries. A good SOC is one that supports business objectives and effectively improves a company's risk posture. A truly effective SOC is one that provides a safe environment for the business to deliver on its core objectives in line with its strategic direction and vision.

A well-designed and implemented SOC can maximize existing security investments by linking individual technical components (such as anti-virus, IPS, IDS, etc.) in a manner that extends the benefits these systems bring in isolation.

Less than 20% of organizations have real time insight on cyber risks.

42%

of respondents don't have a SOC.

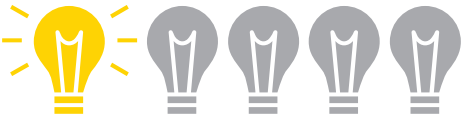
Whether an organization is building a new SOC or looking to expand existing capabilities, here are 10 considerations for success:

1	Executive and board support
2	Investment
3	Strategy
4	People
5	Processes
6	Technology
7	Environment
8	Analytics and reporting
9	Physical space
10	Continuous improvement

36%

of respondents say that their SOC does not interact with the business.

22% of respondents do not know if their SOC interacts with the business.



20%

of respondents say that the SOC receives **annual** updates from the business to understand and address their concerns and risks.

10% recieve **quarterly** updates.

1 Executive and board support

A bottom-up or grassroots approach to security has a minimal chance of survival and an even smaller chance of success. Without clear executive support, a SOC may be ineffective, and its value will not be realized. Creating a effective SOC requires support to establish a clear charter for the SOC and a long-term strategy, and also a strong SOC leader to drive organizational change and develop a culture of security.

Securing executive support

In your quest to secure executive support, be ready to tell a compelling story. Here is how you can structure this important discussion.

Define problems and impacts

- A Why do we need a SOC?
- What issues will the SOC solve for the organization?
- What must the SOC accomplish to solve the existing problems?

Demonstrate vision

- What is your short-term vision?
- What is your long-term vision and how will you meet desired end-state maturity objectives?
- How does your vision align with business objectives, priorities and risk posture?

Know what it takes

- How will you enable the success of the SOC?
- What do you need in order to accomplish the SOC's objectives (people, process, technology, governance, etc.)?
- What should be done in-house and what can be outsourced?

Figure out the price tag

- What is the required initial investment?
- What are the on-going costs of running/evolving a SOC?
- What are others spending in this space?

Quantify the value

- How will you demonstrate the value of the SOC?

2 Investment

One of the most significant challenges SOCs can face is their ability to work (and succeed) within their often limited means, especially when they have not yet developed a track record of success or produced any tangible results. This is particularly difficult in an environment where a significant number of respondents in this year's GISS survey cite budget constraints as their number one obstacle to delivering value to the business.

Within the limited means available, focus on acquiring the right talent. Today's cybersecurity functions require a broad range of capabilities with a diversity of experiences. This may be a difficult task, especially in less desirable geographic locations and given the overall scarcity of experienced SOC/incident response (IR) professionals in the industry. To attract the right talent, organizations will likely need to offer premium compensation and access to growth opportunities.

SOC technology and the operating model will take another large bite from the budget. Open-source tools are free to use, but will require advanced practitioners to customize and operate them.

Vendor-supported solutions are easy to use but come with expensive licensing and support fees. Given these two extremes, it's important to find the right balance that makes the most of limited funding. Allocate resources to secure some quick wins and demonstrate value to the business: this will lay the groundwork for increased investment in the future.

63%

of GISS respondents cite budget constraints as the main challenge to the Information Security function's contribution to the organization.

53%

also cite the lack of skilled resources as a barrier to value creation.

Say it and prove it

The conversation around funding for security monitoring and IR efforts must reach beyond IT and into the executive suite. Once the Information Security function has a seat at the table, it needs to tell a compelling story.

Our experience indicates that board members are more convinced about the need to do something when the story includes:

1) **An independent security program review that can assess security risk and overall maturity of the security function**
2) **A scenario-based assessment that translates technical issues into high-impact business risks**

Broad-scale security assessments can identify desired improvement opportunities based on overall maturity of the security function and risk appetite of the organization. However, where traditional security assessments can fall short is in making the findings relevant to the business. Benchmarks alone are no longer a compelling driver for change and maturity is a relative concept. Organizations also need to move beyond compliance and look at security through the lens of performance and value.

58%

of respondents say that business continuity/disaster recovery/resilience topics are regularly presented to the top governing structure of the organization, but only 14% present SOC metrics.

3 Strategy

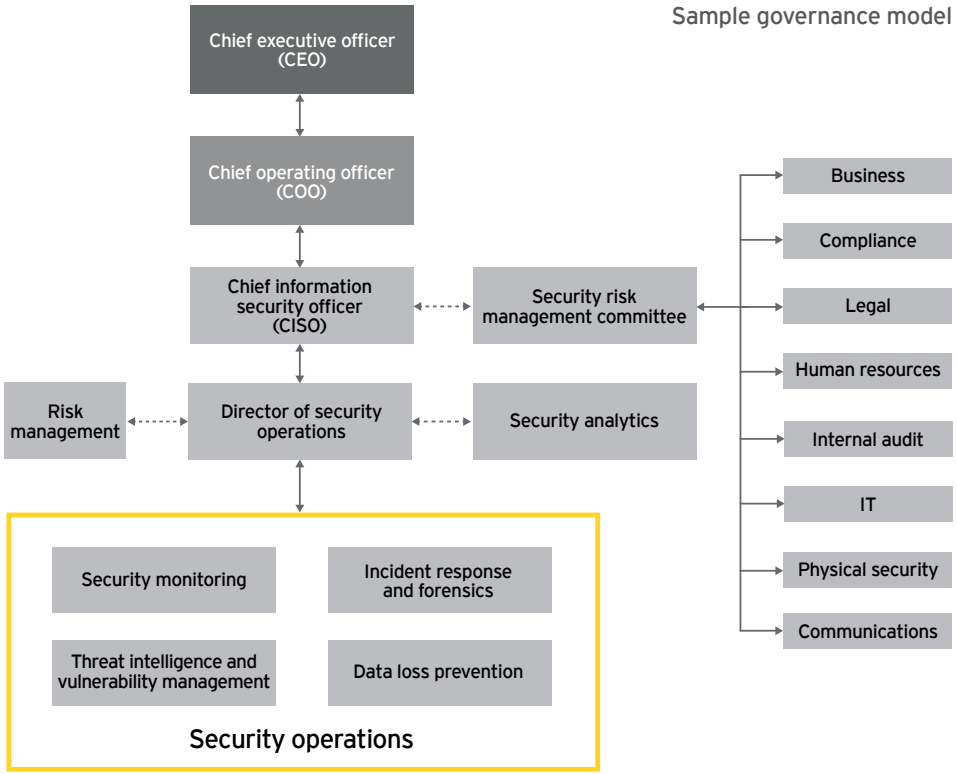
A SOC must be able to clearly articulate its vision, mission and objectives within the context of three critical priorities:

1. Alignment with overall risk posture
2. Support of business goals
3. Assistance in meeting compliance obligations

To gain support and commitment, SOCs must serve as shared service centers that deliver meaningful value to business stakeholders that aligns with their interests. As an inherently cross-functional organization, its introduction sometimes involves aggregating and centralizing existing operations from disparate departments. The failure to intelligently reassign and reorganize these resources and processes represents a common pitfall that can jeopardize the success of a newly established SOC before it even commences operations.

To this end, organizations need to thoroughly define and formalize the SOC's governance and operating model (along with documented service-level agreements and processes) to achieve accountability and oversight, manage communications and guide timely interactions with relevant functions such as IT, IR, HR, legal, compliance and others. A clear chain of authority can also minimize confusion and uncertainty during high-impact emergency actions (e.g., system shutdown and connectivity termination).

Sample governance model



Additionally, organizations need to develop a governance framework for elevating security issues and evaluating their impact on the business. Policies and standards are fundamental to establishing a security-focused culture and enabling lasting organizational change. Policies define the organization's long-term strategic vision and position on key matters while standards provide the tangible implementation guidance to enforce those rules; together, they lay the foundation upon which all other initiatives are measured in terms of value, alignment and prioritization.

Most importantly, without policies and standards, the SOC has no authority to take action in response to findings; attempting to enforce rules without clear guidance to employees can put an organization in trouble from a legal standpoint (e.g., HR complaints, wrongful termination). Without policies, the notion of inappropriate behavior makes little sense to employees and enforcement can leave the organization in a state of confusion and weaker.

Companies must develop a governance framework for elevating security issues and evaluating their impact to the business so that appropriate risk handling can be applied.

Security operations vs. network operations

Security Operations Centers (SOCs) and Network Operations Centers (NOCs) exhibit several similarities. Both functions are frequently organized in a similar fashion using a tiered approach with similar roles at the lowest levels. They both share some tools, although each one also has a unique toolkit and techniques. Both groups leverage deep knowledge of the computing environment and require broad technical skills. What is mostly different is their perspective. While the NOC is primarily concerned with serving the business, the SOC's main focus is to protect it.

When an outage is detected, NOC personnel are likely to attribute the disruption to device malfunction or system issue and attempt to address it through hardware replacement or configuration adjustment. On the other hand, SOC personnel are likely to attribute the problem to malicious activity and will thus prompt an investigation before initiating response actions.

Together, the differences and similarities between the SOC and the NOC introduce powerful synergies that can greatly benefit the organization. Some examples include:

- Improved communications and shared knowledge to enhance situational awareness and response capabilities
- Reduced incident response times by enabling the Information Security function and IT to work together toward common goals, with each contributing specialized skills and experiences
- Improved countermeasure planning though joint accountability for identification and resolution of root causes
- Streamlined incident management reporting with valuable technical context

At EY, we see that information security functions can deliver optimal value when the functions are not embedded within IT. Those organizations that can navigate the political challenges associated with the SOC/NOC partnership can reap significant benefits in the long run.

However, the operating models, processes and procedures of most of today's organizations are still not sufficiently mature enough to support this advanced model of operation.

Don't be afraid to seek third-party support

It takes time to mature a security monitoring operation. During the initial period of rapid growth and development of the SOC, organizations may need some outside help. The right managed security services partner can offer in-depth knowledge and additional skilled resources as the SOC builds its foundation. As internal capabilities mature, the SOC can begin to wean its dependence on the external support over time, eventually phasing it out completely.

4 People

The SOC requires talented resources who possess deep technical knowledge, and also a broad range of capabilities and diversity of experiences. SOC staff should be able to efficiently analyze large volumes of data, intuitively recognizing the need for further investigation. An effective SOC should strike the right balance between security professionals and internal IT transfers who can bring a solid understanding of the company's IT environment and the core business functions the infrastructure supports.

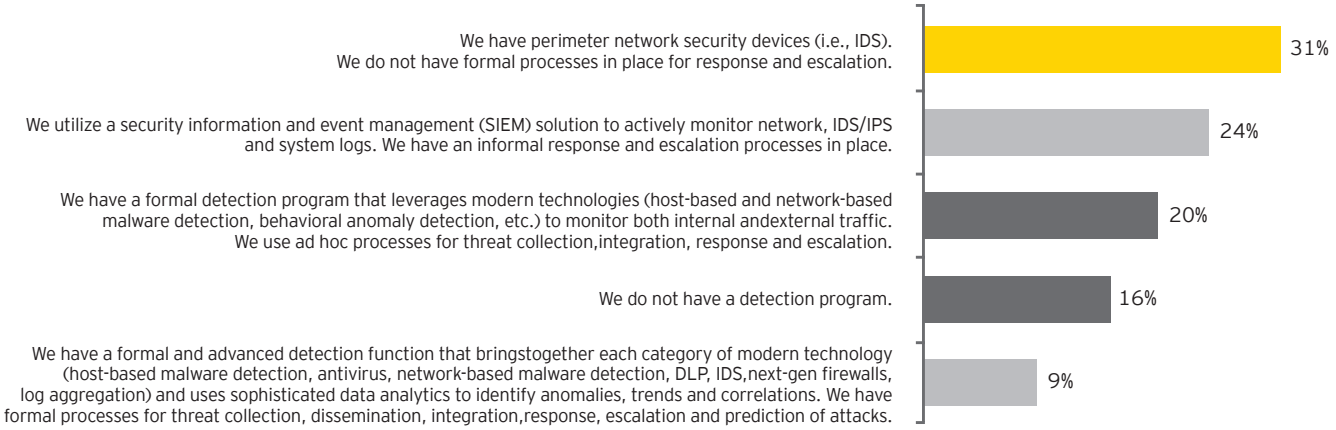
External security hires can bring a fresh perspective based on prior experiences. The SOC may want to augment these resources with less experienced (and less expensive) personnel who can be developed with the proper coaching and mentorship provided by the experienced hires to become seasoned security professionals.

5 Processes

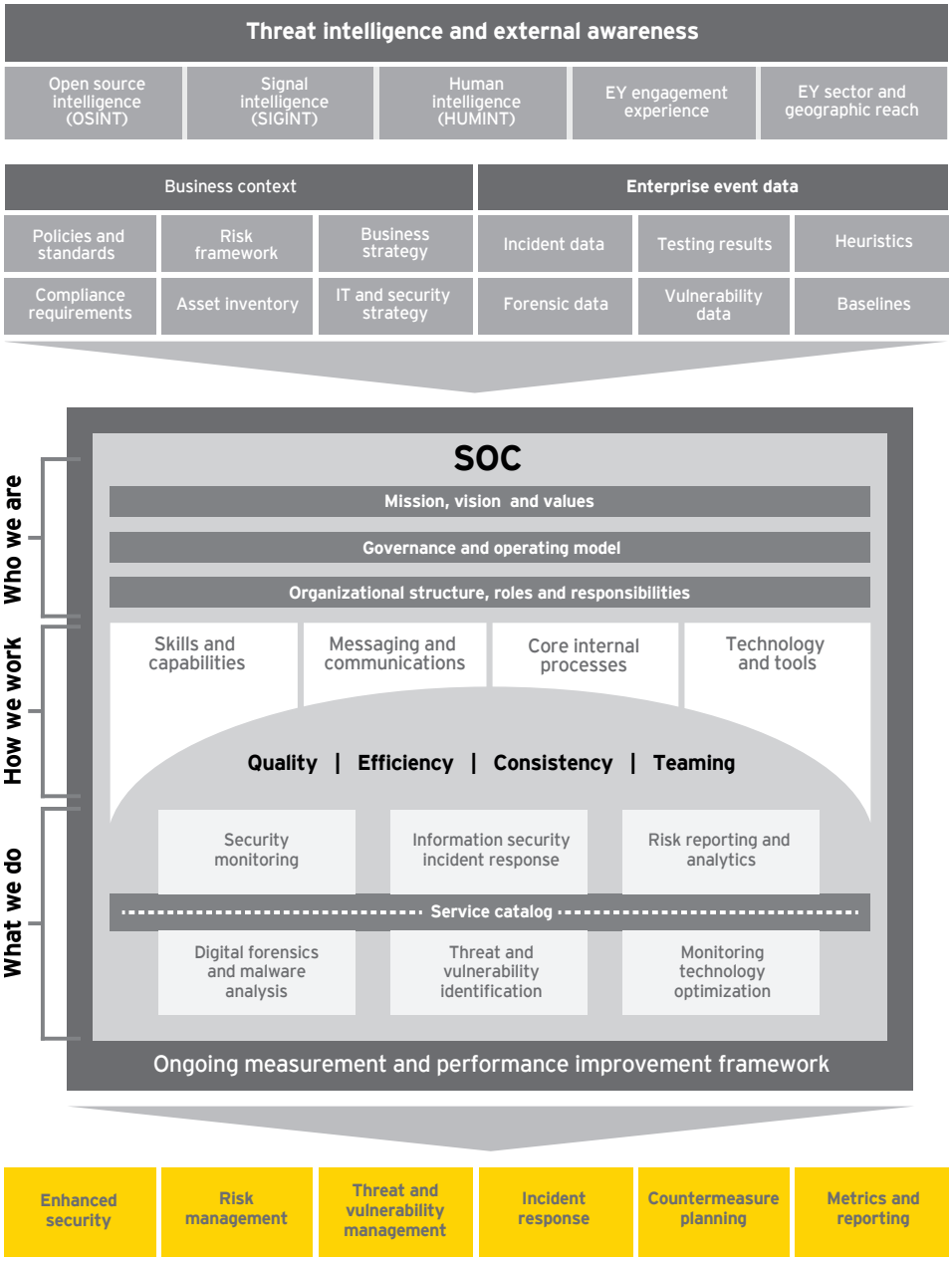
Well-defined processes enable consistent operations and repeatable outcomes. The SOC needs to document and communicate processes effectively and implement change management mechanisms to quickly update processes when improvement opportunities arise.

A SOC also needs to create processes with enough breadth and depth to sufficiently address the universe of possible incident scenarios and provide detailed guidance for response. For example, a SOC must document processes to triage various types of incidents (e.g., phishing, malware infections, BYOD-related incidents, website defacement, denial-of-service attacks) as well as decision guidelines for the appropriate response measures for each (e.g., deployment of incident response team, forensic investigation, malware analysis). The SOC will need to define and implement these processes in collaboration with related departments. Joint planning is essential for a timely and unified response as well as a proper assessment of impact to the organization.

Our GISS 2014 report asked which statement best describes the maturity of your breach detection program?



Forward-looking organizations are designing their SOCs to integrate incident response processes and technical security monitoring systems with emerging technologies in fields such as threat intelligence and security analytics. By designing the SOC with an awareness of these emerging technologies, organizations can spread the investment and add capabilities to their SOC in an incremental manner. A SOC that has been designed in this manner also can be used to more effectively direct related investment costs such as aligning penetration testing costs with quantifiable exposures.



Be aware of the blind spots

Industrial control systems are frequently considered the crown jewels of business operations – yet few pay any attention to them. Most SOCs are still in the process of enhancing monitoring and response capabilities for IT infrastructure and critical systems.

SOCs often exclude operational technology (OT), which includes resources found in SCADA and process control environments, from any security-based checks or vulnerability scanning that is not explicitly required for regulatory purposes. To make matters worse, vendors tend to control patching cycles, and SOCs rarely monitor operational networks for illicit behaviors.

The fear of causing an operational disruption is so significant that the business may react with scepticism and be highly concerned about any attempt to make changes. The result is that these environments remain largely unmonitored, greatly increasing the complexity of security risk management efforts for organizations.

Our GISS 2014 responders typically outsource a range of SOC functions. Of those that have a SOC:

- 32% do penetration testing
- 26% have real-time network security monitoring
- 23% engage in vulnerability scanning and management
- 20% fulfill all functions in-house
- 20% use threat intelligence collection/feeds
- 18% undertake incident investigation
- 15% involve digital/malware forensics
- 14% have threat intelligence analysis capabilities
- 7% do cybersecurity exercise creation and delivery

37%

of respondents do not know how their SOC keeps up to date with the latest threats. Others say:

1. Our SOC has analysts that read and subscribe to specific open source resources (33%)
2. Our SOC collaborates and shares data with others in our industry (30%)
3. Our SOC has a paid subscription to cyber threat intelligence feeds (30%)
4. Our SOC has dedicated individual(s) focusing solely on cyber threat intelligence (24%)
5. Our SOC collaborates and shares data with other public SOCs (20%)

6 Technology

Organizations often deploy technology as a means of addressing business or security imperatives. Projects named after technical solutions are frequently measured by the success of the implementation rather than by the value the technology provides. For example, when asked about capabilities around data protection, GISS respondents frequently make references to a data loss prevention (DLP) deployment and place little emphasis on the other components of a DLP program such as policy and standard development; data governance; information asset tracking and inventory; information classification and life cycle management; risk assessments; and supporting processes and procedures for alert handling.

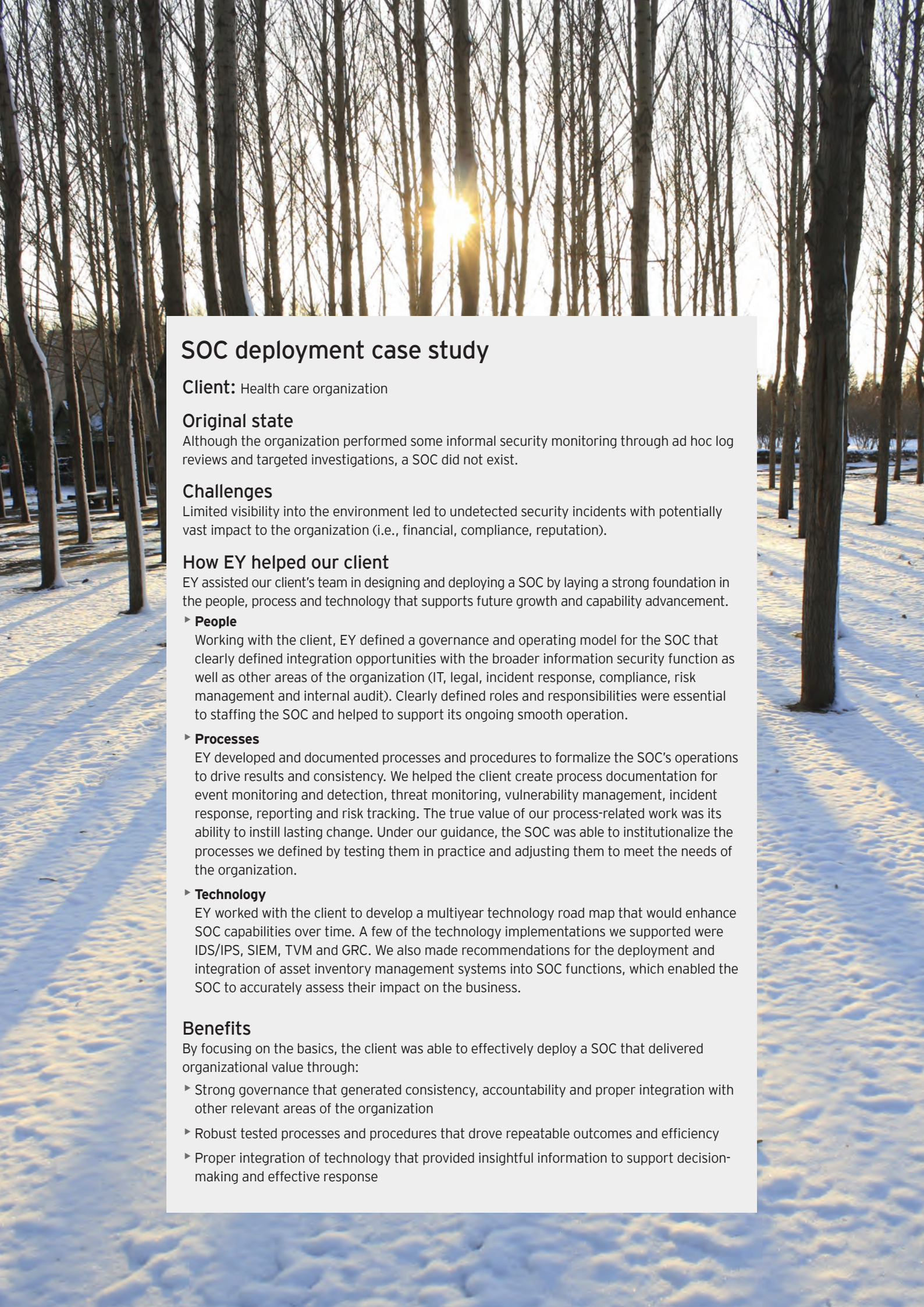
To gain the most value from a technology solution, organizations must supplement their technology deployment efforts with strategic initiatives that address proper governance, process, training and awareness. Similar challenges exist when the rollout of a SOC is equated to the deployment of a SIEM system. The rollout of a well-designed SOC is the step companies must take to reap the most benefit out of a SIEM implementation.

A SOC must be equipped with a suite of technology products that provide the right visibility into the environment commensurate with the organization's security posture. When selecting the right technology, the SOC needs to assign a qualified security team that can identify exactly which tools are right for the job. This team will be responsible for evaluating RFPs from multiple vendors, considering system integration requirements, assessing interoperability with existing infrastructure and conducting solution demos and trials.

Some of the required tools may include intrusion detection and prevention technology; SIEM solutions; threat and vulnerability management tools; filtering technologies; data loss prevention tools; traffic/packet inspection solutions; data analytics platforms; and reporting technologies. In addition, depending on the scope of the responsibilities, the SOC may also have access to other business systems such as enterprise forensic tools in support of incident response investigation efforts.

Although technical tools are important, deploying technology for the sake of technology is costly and ineffective. SOC technology plans should first consider what is available in-house to meet SOC needs: the SOC can then enhance and broaden current capabilities through the deployment of supplemental tools and technologies.

Addressing SOC technical investments as part of the organization's broader IT strategy and portfolio management processes is likely to yield better results than pursuing informal security technology acquisitions in isolation.



SOC deployment case study

Client: Health care organization

Original state

Although the organization performed some informal security monitoring through ad hoc log reviews and targeted investigations, a SOC did not exist.

Challenges

Limited visibility into the environment led to undetected security incidents with potentially vast impact to the organization (i.e., financial, compliance, reputation).

How EY helped our client

EY assisted our client's team in designing and deploying a SOC by laying a strong foundation in the people, process and technology that supports future growth and capability advancement.

- **People**
  Working with the client, EY defined a governance and operating model for the SOC that clearly defined integration opportunities with the broader information security function as well as other areas of the organization (IT, legal, incident response, compliance, risk management and internal audit). Clearly defined roles and responsibilities were essential to staffing the SOC and helped to support its ongoing smooth operation.
- **Processes**
  EY developed and documented processes and procedures to formalize the SOC's operations to drive results and consistency. We helped the client create process documentation for event monitoring and detection, threat monitoring, vulnerability management, incident response, reporting and risk tracking. The true value of our process-related work was its ability to instill lasting change. Under our guidance, the SOC was able to institutionalize the processes we defined by testing them in practice and adjusting them to meet the needs of the organization.
- **Technology**
  EY worked with the client to develop a multiyear technology road map that would enhance SOC capabilities over time. A few of the technology implementations we supported were IDS/IPS, SIEM, TVM and GRC. We also made recommendations for the deployment and integration of asset inventory management systems into SOC functions, which enabled the SOC to accurately assess their impact on the business.

Benefits

By focusing on the basics, the client was able to effectively deploy a SOC that delivered organizational value through:

- Strong governance that generated consistency, accountability and proper integration with other relevant areas of the organization
- Robust tested processes and procedures that drove repeatable outcomes and efficiency
- Proper integration of technology that provided insightful information to support decision-making and effective response

61%

of organizations have not alligned their information security strategy to their risk appetite or tolerance.

51%

of organizations do NOT align their information security strategy with their organization's business strategy.

7 Environment

The overarching purpose of a SOC is to secure and enable the business. To do so, SOC personnel must understand the business and the value associated with specific decisions in order to prioritize the most appropriate response.

To manage events that align to business priorities and assess the true risk or impact to the organization, the SOC needs a well-maintained enterprise asset management system (which includes criticality of supported business processes).

Technical infrastructure knowledge maintained by the SOC, or obtained through close partnership with IT, is critical to the SOC's success. For example, investigating all activities that seemingly deviate from the norm is inefficient and costly; however, environmental baselines can assist the SOC in prioritizing vulnerability remediation or event resolution based on business imperative.

The two factors – business knowledge and infrastructure familiarity – are immediate benefits that internal transfers bring to a new SOC. Furthermore, requirements from policies and standards can help align SOC operations to the organization's overall risk and compliance posture by detecting and resolving high-risk behaviors and policy/standards violations. By correlating business-relevant information against available technical data, the SOC can produce security industry trends that can enable the business to improve decision-making, risk management and business continuity.

8 Analytics and reporting

Today's SOCs have the arduous task of monitoring enormous volumes of data to find those pieces of relevant information that signify an event worthy of action or further review.

Signature and rule-based tools are no longer as effective in the current environment and new threat models have rendered the concept of the "defensive perimeter" obsolete. The SOC can bring unique value to monitoring activities by using behavior-based analytics against environmental baselines. By using advanced techniques, the SOC can analyze data across various systems and devices, providing visibility into unique trends and patterns that may have been obscured otherwise.

The SOC can also use analytics to create insightful metrics and performance measures. It can use some metrics to facilitate operational improvements internally, while management can use others to make more informed decisions when balancing the trade-offs between cost and risk. Thus, a thoughtful metrics and reporting framework can add value beyond security matters by also serving as a compelling communication vehicle for financial and operational concerns.

9 Physical space

The SOC should maintain its own physical space in a secure facility. Creating a distinct location for the SOC, along with the requisite hardware and software, will facilitate shorter response times and promote unity, knowledge-sharing and closer teamwork.

SOC analysts rarely work in isolation. Harnessing the diverse, collective knowledge and experience of the team can be far more powerful than that of any individual alone. SOC analysts also perform most effectively when in physical proximity to each other. Successful SOCs with a high degree of teleworking are exceedingly rare. For these reasons, the SOC should include a facility design that encourages collaboration and resembles an interactive "war room" rather than individual cubicles.

10 Continuous improvement

Just as security is ever-changing, the field of SOCs must evolve as well. Organizations must establish a framework for continuously monitoring performance and improving their information security programs in the areas of people, process and technology.

The SOC needs to provide proper education and on-going training so that the skills and knowledge of its people can evolve with the changing threat landscape. Similarly, processes will need to adapt to deliver greater value. Finally, the SOC will need to constantly evaluate technical capabilities to assess their relevance and effectiveness against evolving internal and external threats.

These factors should be inherently built into the design of the SOC organization and its operations. For example, following the conclusion of a major incident or unique investigation, "after action" reports and "lessons learned" debrief sessions identify opportunities for improvement, keep management informed and recognize the contributions of the SOC and interdepartmental team members.

On average, how long does it take a SOC to initiate an investigation on discovered/alerted incidents?

Within 10 minutes: 12%

Within an hour: 25%

Within four hours: 13%

Within a day: 13%

Longer than a day: 4%

Unknown (or did not answer): 33%

Organizations must be prepared to combat against, and manage and mitigate cyber attacks that can occur anytime, anywhere.

A SOC helps manage cyber threats

The blistering pace of technology change and the cyber threats that come with it are only going to accelerate.

A SOC gives an organization the ability to anticipate and respond more quickly to threats, work more collaboratively and share knowledge more effectively. The SOC can act as a security-monitoring, detection and response hub for the entire enterprise.

But for such a facility to be truly effective, it requires a commitment and accountability at the board level – without it, the SOC can never realize its full potential.

A successful SOC is a strong foundation for operational excellence driven by well-designed and executed processes, strong governance, capable individuals and a constant drive for improvement.

Do's and don'ts for getting started:		
Do	get your executive leadership team on your side.	✓
Don't	understate the full cost of building a SOC. Avoid surprises and hidden costs and communicate openly to secure the needed funding.	✗
Do	develop strong governance processes for accountability and oversight and define rules of engagement with other areas.	✓
Do	build a capable team.	✓
Don't	start with the technology. Understand your needs first and then find technical solutions (new or existing) that fit.	✗
Do	enable repeatable outcomes through formal processes, procedures and protocols.	✓
Do	understand your most prized assets and tailor SOC operations accordingly.	✓
Do	use available information to enhance decision-making and response efforts.	✓
Don't	underestimate the value of collaboration. Build a work environment that fosters teamwork and enables effective operations.	✗
Do	keep up with the ever-changing threat landscape through continuous improvement practices.	✓

Want to learn more?

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our ***Insights on governance, risk and compliance*** series at ey.com/GRCinsights

Get ahead of cybercrime: EY's Global Information Security Survey 2014
www.ey.com/GISS2014

Achieving resilience in the cyber ecosystem
www.ey.com/cyberecosystem

Reducing risk with Cyber Threat Intelligence
www.ey.com/CTI

Cyber program management: identifying ways to get ahead of cybercrime
www.ey.com/CPM

Privacy trends 2014: privacy protection in the age of technology
www.ey.com/privacy2014

Maximizing the value of a data protection program
www.ey.com/dataprotect

Identity and access management: beyond compliance
www.ey.com/IAM

Building trust in the cloud: creating confidence in your cloud ecosystem
www.ey.com/cloudtrust

Big data: changing the way businesses compete and operate
www.ey.com/bigdatachange

At EY, we have an integrated perspective on all aspects of organizational risk. We are the market leaders in internal audit and financial risk and controls; and we continue to expand our capabilities in other areas of risk, including governance, risk and compliance as well as enterprise risk management.

We innovate in areas such as risk consulting, risk analytics and risk technologies to stay ahead of our competition. We draw on in-depth, industry-leading technical and IT-related risk management knowledge to deliver IT controls services focused on the design, implementation and rationalization of controls that potentially reduce the risks in our client's applications, infrastructure and data. Information security is a key area of focus where EY is an acknowledged leader in the current landscape of mobile technology, social media and cloud computing.

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

EYG no. AU2689
ED none

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/GRCinsights

About EY's Advisory Services

Improving business performance while managing risk is an increasingly complex business challenge. Whether your focus is on broad business transformation or more specifically on achieving growth, optimizing or protecting your business, having the right advisors on your side can make all the difference.

Our 30,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and exceptional client service. We use proven, integrated methodologies to help you solve your most challenging business problems, deliver a strong performance in complex market conditions and build sustainable stakeholder confidence for the longer term. We understand that you need services that are adapted to your industry issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where your strategy and change initiatives are delivering the value your business needs.

To find out more about our how Risk Advisory services could help your organization, speak to your local EY professional or a member of our global team, or view: ey.com/advisory.

Our Risk Advisory Leaders are:

Global Risk Leader		
Paul van Kessel	+31 88 40 71271	paul.van.kessel@nl.ey.com
Area Risk Leaders		
Americas		
Amy Brachio	+1 612 371 8537	amy.brachio@ey.com
EMEIA		
Jonathan Blackmore	+971 4 312 9921	jonathan.blackmore@ae.ey.com
Asia-Pacific		
Iain Burnet	+61 8 9429 2486	iain.burnet@au.ey.com
Japan		
Yoshihiro Azuma	+81 3 3503 1100	azuma-yshhr@shinnihon.or.jp

Our Cybersecurity Leaders are:

Global Cybersecurity Leader		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Area Cybersecurity Leaders		
Americas		
Bob Sydow	+1 513 612 1591	bob.sydow@ey.com
EMEIA		
Ken Allan	+44 20 795 15769	kallan@uk.ey.com
Asia-Pacific		
Paul O'Rourke	+65 6309 8890	paul.orourke@sg.ey.com
Japan		
Shinichiro Nagao	+81 3 3503 1100	nagao-shnchr@shinnihon.or.jp