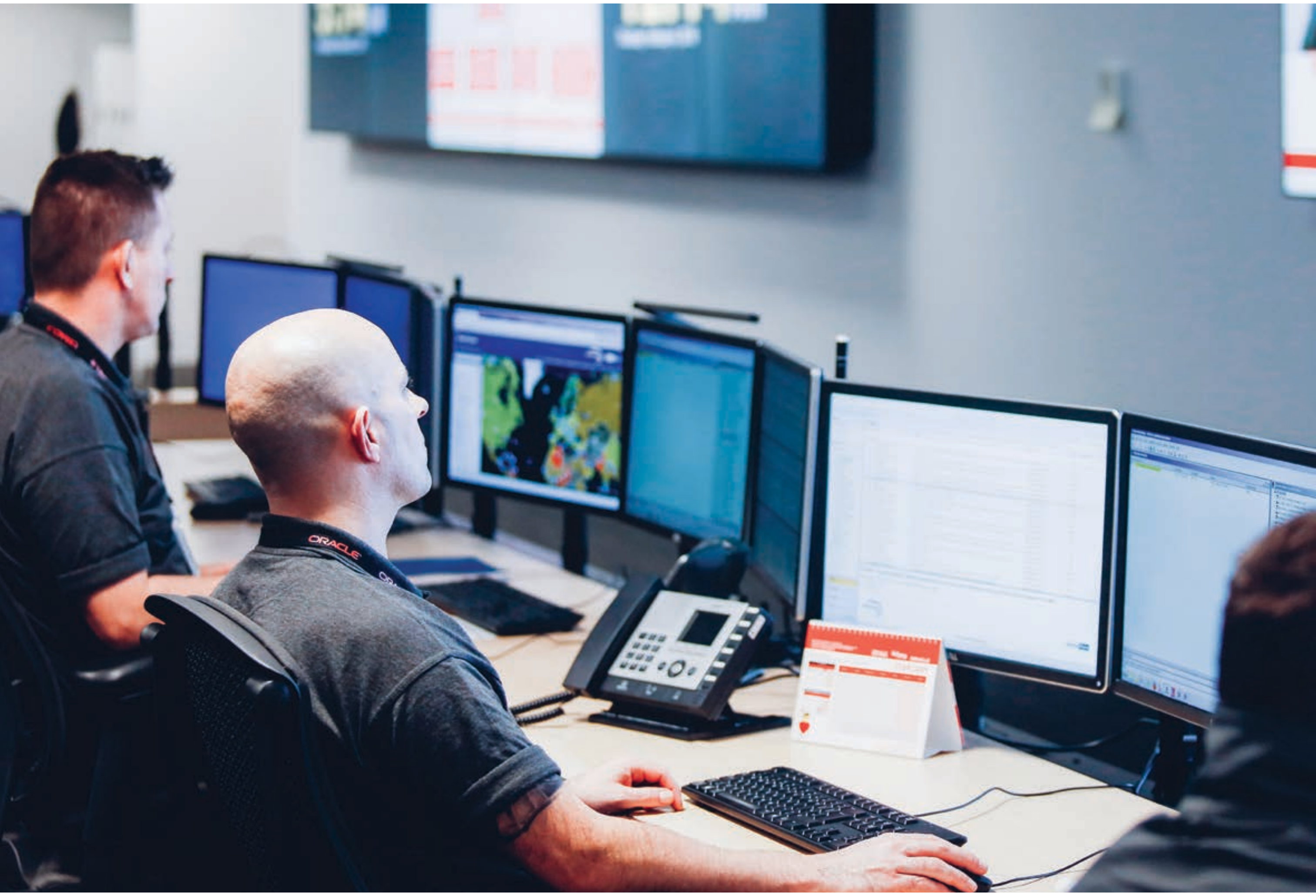
Strategic Plans for Long-Term GSOC Success



By Claire Meyer, Managing Editor

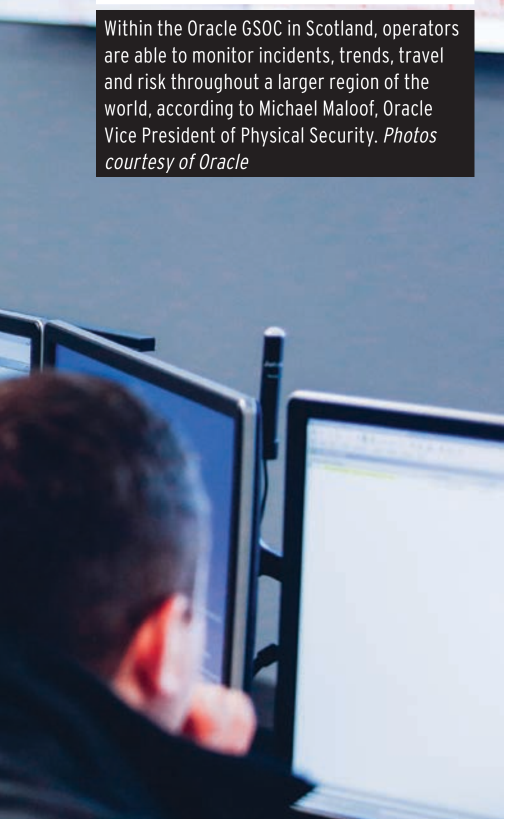
There's no doubt that GSOCs are a massive investment to create and maintain, but how can enterprise security leaders use them to create new value for the business?

Establishing a Global Security Operations Center (GSOC) may seem like a daunting task, given the utter complexity of pulling together so many disparate lines of intelligence, security systems, travel tracking and more. But then enterprise security leaders face the bigger challenge: funding it over the long-term.

The key on both counts, says Brad Minnis, Senior Director of Corporate Safety & Security for Juniper Networks, is staying focused on your mission. Juniper has both a corporate GSOC in its Sunnyvale, California, headquarters and a regional SOC in Bangalore, India, to coordinate worldwide monitoring and incident response.

"Every company is different, so the priorities for the GSOC will be different based on the industry you're in, the assets you have, what culture you're in," he says. When it comes to technology, services and cost-effectiveness, "it starts with is a focus on what your priorities and objectives are for your particular organization. In a lot of GSOC environments, people try to do too much, so you end up overloading the GSOC with meaningless information."

Michael Maloof



Within the Oracle GSOC in Scotland, operators are able to monitor incidents, trends, travel and risk throughout a larger region of the world, according to Michael Maloof, Oracle Vice President of Physical Security. *Photos courtesy of Oracle*

From that mission, Minnis and his department create and revise three-year strategic plans annually for the GSOC, looking at what needs to happen as an organization to keep up with physical security, health and safety needs. When a purchasing decision or operational change comes up, it can always be weighed against that three-year plan to determine if it's a worthwhile investment for the mission of the GSOC.

"The whole idea behind the GSOC is we want to keep our assets out of harm's way," says Steven Ibison, Chief Security Officer for Noble Energy. "We want to maintain constant awareness of all our assets. We want to be able to identify and communicate the threats that we see coming into the GSOC, and we want to mitigate that risk by keeping people out of harm's way."

Noble Energy is a natural energy exploration company, with operations in Israel, Cypress, Egypt, Mexico City, West Africa, the Gulf of Mexico, Colorado and West Texas. The GSOC is located in the Houston hub, but a smaller SOC is located in Tel Aviv. When Ibison came onboard as Noble's first CSO in 2013, it quickly became obvious to him that there was no way to centralize communications, so if something were occurring in the Eastern Mediterranean, it was unlikely that executives in Houston would know about it, at least not quickly. By utilizing a GSOC that manages emergency communication, threat monitoring, enterprise access control, security video and more, Ibison's team can keep leadership and stakeholders informed of developing incidents with hour-by-hour updates to better inform their decision-making.

For example, in a 2014 conflict along the Gaza Strip, missiles were being shot into Israel. Through the GSOC, Ibison and his team kept key leaders informed and aware of any new developments. "We are the largest producer of natural gas in Israel," Ibison says. "It's very important to our company that this continues, and we need to keep our business leaders here in Houston aware so they can make those important decisions."

For Oracle Corporation, the construction of its three GSOCs – one for the Americas; one for Europe, Africa and the Middle East; one for Japan and Asia – involved closing around 20 regional operations centers to unify threat analysis across entire regions, not just countries, giving Oracle a "true global picture," according to Michael Maloof, Oracle Vice President of Physical Security.

"As the world begins to experience some of these unfortunate events, whether it's terrorism or acts of war, we're able to view how those situations impact not just a single site or a single city but an entire region for Oracle," he says. "And where that really comes into play is for our travelers – they may be traveling through a region or visiting a new city, and the Oracle GSOC helps manage our travelers, mitigate any potential issues, and if an unfortunate incident occurs, we can reach out to employees and travelers in a particular region and verify their welfare and check on their status. Not only that, but provide them next steps. Do we want them to leave the country, is it safer to stay in their hotel, etc… Having GSOCs in those areas helps by giving our employees a single number to call for any issue they might have."

Simplify, Simplify, Simplify

If the world were run by engineers and technicians, there would be sensors and alerts on every piece of machinery, and the sheer noise would prove unmanageable for even the most robust GSOC, says Minnis. When it comes to selecting the technology and services provided by your GSOC, "Simplicity is key."

The key to a successful GSOC is staying focused on your mission, says Brad Minnis, Senior Director of Corporate Safety & Security for Juniper Networks. *Photo courtesy of Brad Minnis*

He adds: "We try to standardize how we present information to operators so it's easy to interact with the technologies we may have in the GSOC, and there's a limit to the number of technologies you have to learn to operate… There's a tendency to put in technology that monitors everything, but the operator is presented with a lot of stuff that's actually meaningless. Of all the information that's displayed in a GSOC to an operator, in my opinion, 60-70 percent is not valuable. How do you minimize the amount of information that's not useful and focus on what's most important and actionable?"

It's essential to review the systems in operation at any given time regularly, he says. As technologies and systems develop, they may start overlapping with other programs in use, and then enterprise security leaders can consolidate. Say, if the next generation of your enterprise access control technology gains functionality for visitor management and employee access requests, do you need disparate systems for the latter two functions? "What we look to do is reduce or consolidate the overall number of deployed solutions to make the most of our investment and also reduce maintenance cost on tools that are redundant," Minnis says.

To stay informed on security technology's evolution, Minnis has a "tech guru" on his staff who attends ISC West, ASIS and technology provider events and learns where technology is headed over a three-year period, which helps to drive and inform the department's strategic planning. Having a dedicated technology expert also helps when coordinating security technology installations and maintenance with IT, Minnis adds.

At Amazon, the Business Assurance Center serves as a GSOC, but with additional emphasis on customer service and business enablement. According to Scott Jones (left), Head of Global Threat Management, and Nate Nguyen, GSOC Manager, sifting out nuisance alarms can free up analysts' time for better customer focus. *Photos courtesy of Nguyen and Jones*

When it comes to adding new technologies, "there's a significant amount of time that we're evaluating the product, talk to people using it, visit other locations where it's in use, determine how it may add value to our operation… there's a relatively rigorous evaluation project before we make a significant investment for a global deployment."

"Technology can change overnight," says Ibison. "There's always something better out there. We are constantly looking at new technology, pricing new technology. You can always go out and buy the new shiny thing, but that's not always what you need. We're always staying focused on what the mission of the GSOC is, staying within that box, and looking at the technology that will get us there – it's not always the most expensive technology, but it's what can get us there."

Ibison utilizes Everbridge's Critical Event Management platform and Visual Command Center to overlay multiple intel streams and feeds into one common operating picture for GSOC analysts. "We're not a big company, and I can't hire five or six guys to sit down there 24/7, so one or two people needed to be able to monitor all that at all times, so they can tell me that if there's someone traveling from Egypt to Paris tomorrow that there's nothing going on in either place that would hinder those plans or that traveler," he says. "Most people are visual; with this system, analysts can go down and put up pictures on the screen of where everyone is, globally, where aircraft with our personnel are, weather patterns, protests or airline strikes… overlapped on these maps to give us a quick, down and dirty assessment of what's going on."

"We've gone away from CCTV walls of different sites, and we've gone to a picture of the world – in terms of where are our travelers, where are our employees, what are the threats for an area, what's the crime profile – and getting real-time analytics… that's where we're focusing our GSOC operations," says Maloof. "Let's say that a terrorism incident occurred in XYZ city and we have 13 employees there. Our tools prioritize that as something we need to act upon immediately. At the same time, the press of one button will tell us all the employees and travelers we have in that city, and you click another button and our employee notification system begins to activate and verify the welfare of every employee noted. In the past that was a very intensive process that involved constantly looking at newsfeeds and where that is in relation to sites, where we have travelers, etc. As this technology expands and improves, we would anticipate a manpower reduction as a result."

A New Kind of GSOC Operator

While technology is altering the number of operators needed to maintain situational awareness and response in a GSOC, it's also changing the type of operator that enterprises need.

"What we are looking for in a GSOC operator has changed," says Maloof. "Customer service is paramount. When somebody calls security, they're typically having a bad day at work, and we want to eliminate that potential problem for them and resolve it as quickly as possible. But also having somebody with a wider worldview of what's occurring… An excellent security officer is not necessarily an excellent GSOC operator. We're looking for a new skillset more closely aligned to a threat analyst position. In our Colorado center, we want someone who knows the United States very well, is familiar with Latin America, is familiar with how travel occurs – you should know that Dallas, Houston, Atlanta are major airline hubs… We're looking at folks that understand geopolitical issues, understand customer service, understand how the world operates: Are you familiar with various news sites? Are you aware of events occurring in the world? We've seen that change in recent years, and it puts the pressure back on our contract provider to find the appropriate level of staff. We're finding there are folks from the military – we're a huge proponent of military hire (we have program in place with Warriors in Transition), and that's a great resource for us."

Adds Minnis: "Regardless of the technology that you use, you've got to take into consideration the personnel you use to operate those systems. A lot of companies spend millions of dollars on technology and then put a minimum wage security officer behind the desk to try and manage it. It's critically important that you align the capabilities and skill levels of people you have in place in your GSOC to effectively manage your systems."

The Business Assurance Center (BAC) at Amazon functions, essentially, as the GSOC for Amazon Corporate Security (ACS). The BAC is an integrated part of Amazon's Global Threat Management (GTM) team whose promise is to preserve life, protect assets and promote community, says Scott Jones, Head of Global Threat Management for Amazon. Contract GSOC analysts and in-house

Can a One-Page Document Revolutionize Emergency Response?

Nielsen Holdings PLC, as the world's leading consumer measurement firm, is first and foremost a data-centric company. Nielsen collects information about consumer spending, TV viewing, online activity and more in 106 countries worldwide in hundreds of facilities. Some of those facilities are not heavily capitalized – just a few employees with laptops – so they have the ability to pack up and move in the event of an emergency. However, with such a wide and agile footprint, Nielsen had to think outside the box when devising cost-effective emergency management plans that can succeed without a formal GSOC.

Robert Messemer, Chief Security Officer for Nielsen Holdings, worked with his global team to develop a one-page guide to be used by all office managers around the world, outlining what they need to do in the first hour, first eight hours and first 24 hours after any crisis or business interruption. It lists what to do and what not to do when evaluating and triaging an event, how to work with local first responders, what to share with media, and – vitally – where their priorities should be.

"Our document establishes priorities for the local manager," says Messemer. "Philosophically, it places the primacy of people over operations. It's important for our leaders to understand what the impact of any given business interruption is for our people, and what we are doing to either account for missing people and to make sure we are doing all we can do to assist them. It's an important initial phase in our response to whatever business interruption is taking place."

He adds: "One of the reasons we put this in play 10 years ago is that we found many of our leaders wanted to do the right thing, but sometimes they prioritized business operations and getting systems back online ahead of ensuring that our people were well and accounted for. We wanted to make sure that given any bad situation, even with the best of intentions, there wasn't a bad situation that now became worse."

"It's important for our leaders to understand what the impact of any given business interruption is for our people, and what we are doing to either account for missing people and to make sure we are doing all we can do to assist them," says Robert Messemer, CSO for Nielsen Holdings. *Photo courtesy of Robert Messemer*

For example, during the September 2017 earthquake in Central Mexico, core infrastructure assets (cell service, landlines, electricity) deteriorated or were eliminated. However, the Nielsen office had satellite phones assigned to it, so leaders there could have instant communication with key personnel at Nielsen's headquarters. News could be shared with stakeholders through a regularly updated Google Doc to keep everyone up to speed. During the crisis, the managers referred to the one-page document, which instilled a sense of confidence in knowing the next steps.

To ensure that the situation doesn't deteriorate further and guiding principles are followed during the 24 hours after an incident, the document might provide guidance regarding:

- Finding employees and seeing to their immediate needs
- Providing care for employees, their families and stakeholders
- Finding and securing assets (after securing people)
- Determining any client impact
- Determining what resources are needed for associates and extended stakeholders
- Determining what action is required to restore business operations

Having these actions taken on the ground helps the Nielsen corporate crisis management team obtain the right information immediately and move forward on restoring operations more effectively and efficiently.

"We in the Nielsen security team take a lot of pride in the services we provide and the immediate positive impact we can make in any business interruption." Messemer adds.

Messemer also works to ensure Nielsen's leaders are up to date on emergency procedures, but he notes that, due to the political climates in many of the countries where Nielsen works, many managers have abundant real-life experience with unforeseeable business interruptions. "With the Mexican earthquake, it turned out beautifully, and the feedback we received from the executives on-site was simply they never appreciated the pre-planning that went into the plan, until the quake happened. Their first instinct was to go back to their training, which was to refer to the emergency response document and to begin to execute. It gave them such a sense of confidence. What I have found is that executives who have practiced this in real life in one market, as their careers progress to larger markets, they take their experience and insights. For example, as someone progresses in their career as managing director in Istanbul, Turkey, to a larger role in Paris, Moscow or London, they take these important insights with them into their new roles. Our leaders demonstrate confidence knowing that our emergency response plans worked in other markets."

After an incident, the security team gathers feedback on what worked well and what could be improved, and the response shows how having a people-centric emergency response plan resonates with Nielsen employees.

"Another benefit is that our emergency response plans foster greater collaboration and employee engagement. Our associates were so appreciative of the fact that anybody in the company even gave thought to this, that we're putting people first – not operations, not clients' deliverables – they have really responded favorably to it. Our associates view security in a different context," Messemer says. "Instead of being contacted by security being perceived as being contacted by HR – often interpreted as a negative thing – the perception of security changes to something really positive. Security may be viewed as being a little paternal, but it's a very favorable change. Our plans energize our people who are eager to collaborate and offer suggestions on training or altering our plan depending upon prospective business interruptions or different political risk scenarios."

security personnel manage a high volume of alarms, field calls about security issues and provide customer service to internal clients.

"As security technology advances to help mitigate nuisance alarms, it unlocks analyst time and allows more focus on customer service. Internal customers will rarely interact with the GSOC for security-related issues, but will often reach out for support for simple things like help with finding lost keys or getting access to a parking garage. These seemingly small interactions are incredibly important and serve as the first opportunity for the BAC to earn trust with its partners," says Nathan Nguyen, GSOC Manager.

Early on in the life of the BAC, Jones decided to take a different route when hiring. He looked for potential hires with backgrounds in hospitality and journalism, in addition to traditional security personnel. "A diversity of skills, opinion and thought processes allows us to have a stronger product in the end," he says.

Marketing the GSOC

There's no question that a GSOC is an expensive investment, but cutting costs isn't necessarily the best way to make it worthwhile to the enterprise. Technology can reduce the number of operators needed around the clock, and some services have tangible ROI, but getting buy-in hinges on communicating those benefits effectively, and continuously looking for new opportunities to provide value.

"Thinking of it as a budgetary black hole shows a lack of creativity in marketing your security operations center," says Jones. "Make your GSOC bigger than security – it's not just an alarm shop; you have more capabilities, so market those as an employee benefit. Look beyond the term 'security' even, because most GSOCs are doing more."

In marketing the BAC, Jones and Nguyen took cues from previous experiences within entertainment (Jones) and technical (Nguyen) industries. They take a multi-modal approach to communications and marketing by leveraging myriad internal resources to support education and socialization benefits and services. Creative approaches include the use of infographics for analytics, videos and stakeholder tours of the BAC. Their goal is to not only explain security to employees through the lens of the BAC but to make the center as real to people as possible.

"Technology can change overnight," says Steven Ibison, CSO for Noble Energy, about finding the right solutions for the GSOC. "We're always staying focused on what the mission of the GSOC is, staying within that box, and looking at the technology that will get us there - it's not always the most expensive technology, but it's what can get us there." *Photo courtesy of Noble Energy*

"Whatever operations center you have will tell its own story," Jones says. "Try to break the mold and learn from how other industries market their services. Seek opportunities to tell your story more creatively. And while we cannot be prophets of our own story, we can evangelize through other departments and customer impressions. Whatever you do, obsess over your own customers – not the competition!"

Marketing the GSOC doesn't need to be complicated. At Noble Energy, Ibison gives GSOC tours to the Board of Directors, executives and other stakeholders. "A lot of times folks within your own organization don't realize all the big things and little things that a GSOC brings to the table. We want to let folks know," he says.

Oracle also offers GSOC tours, and Maloof has a dedicated education and awareness manager for the security department who helps to discuss the GSOC and its services at Oracle events or team meetings. "We ask attendees at these sessions to think about their lines of business, and if there's anything the GSOC could do to help support them. And that has been very well received from the executive level down to individual teams. We have taken on additional roles and responsibilities as a value-add to Oracle, such as our facilities emergency updates, traveler protection… in essence, we are constantly saying that security is a resource to any line of business out there, and between lines of business and security, we put our heads together and ask what else we can take on that would be well-aligned with our GSOC at the same time providing support and relief to some other lines of business."

To calculate ROI, Maloof looks at the intangible benefits such as the peace of mind from having a proactive traveler protection program, as well as the tangible, financial benefits. Each Oracle GSOC has a contract systems and technology expert on staff 24/7 with 100-percent ROI. These experts mitigate and manage alarms that appear to be troublesome or a potential malfunction, often performing a repair from the GSOC through reprogramming or modifying the schedule for a particular alarm, to reduce service call demand. If an on-site technician is needed after all, they can call the GSOC technology expert to get a full briefing of the situation, and both sides will work together to test the technology after the repair, reducing the need for repeated calls to the site.

"The value of a GSOC is overwhelming to an organization, and it is a requirement for any larger security organization," Maloof says. "I fully understand that not everyone has the capital infrastructure to build their own, and there are various ways of outsourcing that, but the old methodology of a GSOC – someone to answer the phone for security questions and mitigating alarms – there's so much more that a GSOC can do, and that's where we've found the real value: supporting the safety and security of our employees globally, from the number of different initiatives, both forward looking and reacting when an incident does occur. That for us is the true value of a GSOC." S