GERNETTE WRIGHT

IT Security Officer
SCHNEIDER ELECTRIC

HEADQUARTERS: Rueil-Malmaison, France

EMPLOYEES: 130,000

REVENUE: $34.17 Billion

Gernette Wright has over 25 years of experience transforming and building cyber security and information systems. He began his career on the technical side of IT, working in various roles around systems administration, and infrastructure management, before moving into more security-focused roles serving as Senior Manager for Security Operations, VP of Information Security and most recently IT Information Security Officer. He explains, "Before I took on security-specific roles, I knew I wanted to understand more than infrastructure operations. The challenging technical aspects brought me into security, the ability to be a part of business enablement keeps me here. I've always resonated with the idea that what we are doing has a bigger purpose."

Over one year into his role as IT Security Officer for the Americas at Schneider Electric, working with the R-CISO, Gernette is responsible for maintaining enterprise-wide information security risk and privacy while upholding the necessary security to support business needs. Gernette breaks his responsibilities down into three specific areas.

The first area of responsibility is internal and external footprints – with responsibilities for areas ranging from incident management to internal security governance. This requires a business mindset to understand both what the security goals are in relation to their footprints, but also aligning those to the what the business is trying to accomplish.

The second area is vendor and customer contractual responsibilities, from the cybersecurity compliance perspective. His team looks at contract language that comes in to make sure it has the proper cybersecurity protocols and language in place. This area also brings with it some level of customer-facing responsibilities that requires interacting with customers to answer any questions on internal security programs and articulate requirements and standards as a company to ensure both parties are protected and also happy. Sometimes that means adopting languages from both parties and finding middle ground.

The third, and the main area where Gernette spends the majority of this time is around the company's M&A information security remediation activities. Gernette comments, "We often acquire companies that are young in their security journey. Part of the process includes a formal security assessment. While going through their remediation program, I try to understand what they're currently doing to see what can be adopted and/or enhanced in order to implement our set of security standards so they meet our level of security. Sometimes they have to build a program from the ground up and sometimes there is some type of program partly built and needs to be matured. I believe it's key to ensure their program is tailored to how they work but also ensure our standard framework is followed to help them mature their security program. Although the goal is meet Schneider's standards, this is their program so my approach is to lead them to a solution, never to just throw something at them and insist that it be implemented."

ADDRESSING CHALLENGES

Threat prevention, particularly ransomware, is a constant challenge for Gernette and his peers, because of the ever-evolving nature and need to constantly be up to date on the latest TTP's. He ensures he is always learning and educating himself to better protect his organization and lead security programs with confidence.

Addressing regulations is another challenge, as frameworks and policies are modified and security teams must keep up to meet compliance mandates. Gernette says, "There's a variety of privacy and security frameworks coming out with updates like CSF 2.0. As an industry it is sometimes hard to staff adequately for response to push those changes through, especially if you were already going through a gap remediation in the last version."

Security staffing is also a challenge across most organizations and Gernette believes that will continue with particular security skillsets being harder to find, especially on the governance side. He says cybersecurity jobs revolve around risk mitigation which involves looking at data, something that is not glamorous and can be tedious, leading to burn out and the lack of interest in pursuing this line of work.

POSITIVES AND NEGATIVES OF ARTIFICIAL INTELLIGENCE

Gernette is excited about the advances in AI, he made the point that AI is not new as it has existed in various technologies for quite some time, such as chatbots, facial recognition, speech recognition, etc. He says it is the advances in large language models powering generative AI such as ChatGPT which are revolutionizing our work and personal lives. Although AI brings many innovative transformations, Gernette warns about the fast rate at which AI is entering the market and if policies and regulations can actually keep up with this. He says, "AI is going to change how we do things, and the way we function. Much like the internet, it's going to be transformative. In the context of work there will be many of positives; one area that comes to mind is staffing. There is always a need in our industry for SOC analysts, AI could help augment some of those higher skillsets needed for forensics and eyes on glass. Imagine if a Tier 1 SOC Analyst could conduct an end-to-end forensics on day #1 just by typing a contextual question into an AI backed search bar or reduce false positives. That would transform staffing and operations in the SOC. This is the type of application of AI that will benefit other areas such as vulnerability management and malware detection and prevention, among others, and improve operations in our cybersecurity space."

However, Gernette says like Newton's Third Law, everything has an equal and opposite reaction, and there are also some negative effects of AI. He comments, "As we learned during the pandemic, there was a mass rush to accommodate remote employees and because of the speed of implementation, proper considerations around security controls weren't taken. The speed that companies are adopting AI might mean businesses may forgo a thorough vetting and testing of critical controls in order to go to market sooner. As we've learned, it's hard to go back and put security in place after the fact. The companies putting AI products out there must make sure they are designing with security and privacy in mind before they go to market."

He continues, "On the cyber defense side, an area of concern is phishing. We've developed our awareness training to teach our employees to be cognizant of spelling, grammar, and email address correctness, however with AI, those emails could be written perfectly. The effectiveness of our standard AT training will become greatly reduced or obsolete; we will need to re-tool ourselves and create better ways to educate our user community. We also need to be aware of the privacy challenges with the use of AI. The US has been slow to adopt privacy regulations, but proper legislation is needed to safeguard privacy information and choices. AI systems needs lots of data for its predictive algorithm, which raises concerns about systems abilities to pull in feeds from many different places, processing, access, and storage of that information."

> *"I believe in mentorship, there's always someone who is smarter and more experienced than you."*

LEADERSHIP STYLE & COMMUNICATION

Gernette leads with a democratic type of style, coaching his team members to achieve their goals, while including them in important discussions so they feel valued. He explains, "I involve my team as much as I can, I believe better decisions and work products are a result of joint conversations from cumulative voices and opinions. As an employee, I like to feel valued and that my work and efforts are appreciated, and putting myself in others shoes, I feel they'd want the same."

In past roles Gernette has presented to boards, something he believes must be approached with strong communication and an open mind. He comments, "I try to get to know the board before I present to them so I can understand how they digest information and what they're looking for. You don't need to be technical with boards, but there is value in showing certain metrics, so they understand what you're actually doing and represent cyber posture of the organization. I present from a business perspective to make sure the information is not falling on deaf ears. It's great if you're able to reuse an existing format and tailor that to your style, but in cases where that does not exist, one approach I've taken is use the board audit-subcommittee as a sounding board. I outline what I'm thinking and then ask them for input to fine tune, and I've found this fostered engagement and they feel invested in security. This may not work for every situation or everyone, but given the accessibility and size of the organization, it was an approach that worked well for me at that time."

GROWING AND LEARNING

Gernette is passionate about education and the need to expose yourself to relevant information to stay up to date through upskilling. He attends industry and leadership conferences to improve his communication, hear from other leaders, and network with the larger community. Having a mentor is very important to his growth, he explains, "I believe in mentorship, there's always someone who is smarter and more experienced than you. It's important to find that person to take advantage of their experience and advice and also be a sounding board for my challenges and goals. I've had a few mentors in my career, and they have been a huge part of my growth. I believe it's important to remain teachable in everything I do, to know when to listen and when to talk, whether it's someone from a different part of the business, in a meeting with peers, work social event, etc. You'd be surprised what you learn by just observing and listening."