Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

LOOKING FOR SKILLS IN ALL THE WRONG PLACES

The cybersecurity skills gap is growing exponentially. Businesses are constantly finding new points of vulnerability as they digitise their processes. Where will the next wave of cybersecurity talent emerge from? And how do we nurture these resources to effectively respond to the evolving nature of cybercrime?

THE CYBERSECURITY SKILLS GAP IS GROWING. HERE'S WHERE TO FIND THE TALENT TO FILL IT.

In the last couple of years there has been much said—and just as much written—about the skills shortage in cybersecurity. This quickly widening gap can be attributed to two influences. On one hand, businesses across all industries are beginning to recognize the need for more robust security measures in all of their increasingly digital processes. At the same time, the skills needed to address these issues are becoming increasingly diverse.

There is less information available, however, as to practical ways in which this gap can be addressed at an organizational level.

We spoke with Jérôme Desbonnet and Mike Turner to understand more about how cybersecurity threats have evolved, and what they're doing to defend them.

Jérôme Desbonnet
Global Cybersecurity Chief Technology Officer (CTO), Capgemini Group

Mike Turner
Cybersecurity Chief Operating Officer (COO), Capgemini Group

UNDERSTANDING HUMAN BEHAVIOUR IN CYBERSECURITY

Cybersecurity is big business, and the sizable paycheck associated with the field is a major attraction for many young programmers. But high staff churn and siloed, incomplete solutions mean that many aspiring security experts are disillusioned early in their careers, or fall into the trap of selling Band-Aids for bullet holes.

As Jérôme says, "It's easy to find a company who can sell in an off-the-shelf cybersecurity solution that addresses one area. But you need corporate knowledge—of the industry, of the business, of the people, and of the culture—to start understanding the total nature of potential threats to an organization. It's a multifaceted issue."

Multifaceted is right. Where networks used to be the single point of entry for security threats, there are now multiple points of entry with the ubiquity of connected devices and cloud-based applications. The upsurge of "Shadow IT" adds another layer of complexity to the problem for many organizations. This is the practice of business units autonomously adopting cloud-based applications and programs on a "per user" basis, without following traditional IT procurement channels. For CIOs and those in charge of security, this means that they lack full visibility of their internal IT landscape - and the threats lurking in its most vulnerable corners.

"Cybersecurity is a vital consideration in everything from email to identity authentication in mobile apps. There's constant pressure for businesses to transform digitally, but there's also a lot of legacy architecture still in play, so there's a lack of integration, and a lack of transparency about where threats exist," says Mike.

His opinion is echoed by Jérôme, who states: "Insider threats, human engineering, user behavior - these are all hazards posed by an organization's people, not by the new technology they're using.

> **"Sometimes cybersecurity means protecting people from themselves.**

But just as human users pose a threat to system security, so the solution appears to lie with finding a diversified resource of security-related and interpersonal skills.

"Technology means that we can automate a lot of high-volume, repetitive processes that used to have to be done manually.

> **But there's now more need than ever before for people who can apply critical thinking and analysis to a problem, "**

people who understand the role of business analysis and user behavior in a cybersecurity strategy," Mike states.

Cyberattacks: big risks for business

In 2015, **300 million** records were leaked and over **$1 billion** was stolen in cybercrimes in the United States. It's little wonder then that the FBI now ranks cybercrime as one of its top law enforcement activities. But in spite of the pervasiveness of cybersecurity threats, many businesses still feel unprepared.

According to the 2015 Global Cybersecurity Status Report from ISACA:

- **83%** of organizations agreed that cyberattacks were a top 3 concern for them, but only 38% of organizations felt they were prepared for a sophisticated cybersecurity attack.
- **86%** of organizations believed that there was a shortage of skilled cybersecurity professionals, but 54% of them acknowledged that it's difficult to identify who has an adequate level of skill and knowledge when hiring graduates for entry-level cybersecurity positions.

> "There is a growing need for diversity in cybersecurity. In terms of skills, backgrounds and gender. Different perspectives and ways of thinking can only strengthen the function."
>
> **Jérôme Desbonnet**

CYBERSECURITY EXPERTS ARE NOT WHO THEY USED TO BE

"There are entry-level positions now in cybersecurity that didn't exist ten years ago", says Mike, whose own security career began in the military and with government agencies.

"There is no such thing as a single "cybersecurity skill"—it's a spectrum."

Cybersecurity touches almost every aspect of modern business and, similarly, business needs are influencing the way CIOs construct their cybersecurity resources. There is a growing understanding that different processes and phases in a project lifecycle require the right security-related skills at the right time.

This is challenging the perception of cybersecurity being a single, highly specialized focus area with many barriers to entry, suitable for only a handful of niche technicians—typically middle-aged white men—with many years' experience tucked under their belts. In many cases, graduates who would excel in a security-related position don't consider this as an option because they don't fully understand what cybersecurity entails, or how their individual strengths could contribute to a team.

"Organizations are seeing the same kind of people with the same skills and the same experience, applying for the same security positions. In fact, what we need are more business analysts, project managers, strategists [and] communicators," points out Jérôme. "There is a growing need for diversity in cybersecurity. In terms of skills, backgrounds and gender. Different perspectives and ways of thinking can only strengthen the function."

Mike agrees, and adds, "We're seeing more women enter the Capgemini graduate program, and people who've come from totally different career backgrounds—teachers, marketers, economists—all of these different perspectives add to our ability to identify risks and solutions."

There is still a clear need for deep technical proficiency with regard to network administration, software engineering, coding, identity and access management, cryptography and scripting. Those working toward a CISSP certification can be assured that their accreditation will still be desperately required in the next few years. But there is also an increasing need for a wider skillset that encompasses aspects like business analysis, problem solving, agile thinking, project management, and strategic thinking.

> "You can learn the technical skills, but without an enquiring mind, and the desire to keep learning, you'll never be able to keep up with the changing nature of the threats we face."
>
> **Jérôme Desbonnet**

"I would go so far as to say," speculates Jérôme, a self-confessed former teenage "hacker", "that curiosity is the single greatest thing you need for a career in cybersecurity. You can learn the technical skills, but without an enquiring mind, and the desire to keep learning, you'll never be able to keep up with the changing nature of the threats we face."

FINDING AND TRAINING NEW CYBERSECURITY TALENT

A broader range of vital skills and expertise is good news for graduates and young professionals considering a career in the cybersecurity field, but it's not making recruitment any easier for HR departments.

The findings from the *2015 Global Cybersecurity Status Report from ISACA* acknowledge that 54% of organizations find it difficult to identify who has an adequate level of skill and knowledge when hiring graduates for entry-level cybersecurity positions.

"The natural place to look for technical expertise is in areas like network administration, but we also need to consider that something like user-education is a necessity. This is more of a communication than a technical field, but it forms part of the wider scope of skills that security teams need to consider," says Mike.

He suggests that organizations can take the first steps toward creating a robust and sustainable internal cybersecurity team by:

- Promoting a clear career path for existing employees looking to move into cybersecurity.
- Creating opportunities for internal apprenticeships and knowledge sharing within cybersecurity to upskill existing resources.
- Collaborating closely with the HR function to strongly identify the business needs for various skills within the cybersecurity function, and establishing the criteria for ideal candidates.

"The Capgemini 5-week Cybersecurity Academy is, I think, a good example of how to upskill people from within your organization," he continues. "This is an intensive, onsite upskilling program that covers a broad range of topics from security monitoring and forensics, to major incident management."

A typical Capgemini 5-week Cybersecurity Academy timetable

Week 1	Security Fundamentals
Week 2	Architecture Overview Risk Assessment & Management Security Governance Security Standards
Week 3	Security Monitoring & Forensics Identity & Access Management
Week 4	Legislation Major Incident Management
Week 5	Cloud Security Data Security

The Academy functions in conjunction with a number of Capgemini's other talent recruitment initiatives, such as their two-year onboarding program and graduate programs. Academy attendees can expect to cover a wide range of cyber and organizational security issues in a highly condensed timeframe.

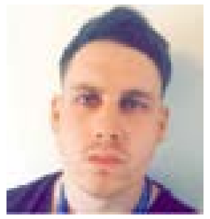
"Obviously this is an excellent "boot camp" for new hires and graduates, but we designed the academy so that it doesn't discriminate on job title or experience," clarifies Mike. That means that everyone from a CIO to an intern can attend the course and glean a better understanding of the cybersecurity ecosystem, and where their skills fit into protecting it.

Capgemini has had great success adopting a rigorous approach to upskilling and finding new talent with its graduate program. Almost 10% of their cybersecurity staff have

"In five years, all but two of the graduates who have joined my team are still on board. In an industry known for struggling to hang on to talent, I think that says something."

Mike Turner

A graduate's opinion: My cybersecurity career with Capgemini



I'd actually been teaching for four years, getting my masters in computing when I applied for the grad program. I'd seen a lot of stories in the media about cybersecurity breaches and it seemed like a really interesting field to get involved in.

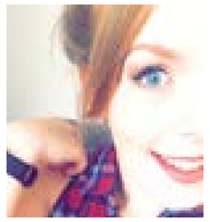
I was put on a graduate rotation, so I could spend four months at a time in any given area in the business. I started doing quite general security work—ISO 27001 reviews, site reviews, security reviews, risk analysis, but then got involved in forensic incident investigation. In one case, there was a systems admin who had gone rogue. The team spent a lot of time on site pulling servers and desktops that might have been involved, doing scanning, log analysis and laptop imaging. That was really technical, and an extremely good learning opportunity for me.

I've been on a lot of courses with Capgemini during the two years I've been here. So in addition to the practical experience offered by the grad program, there's an excellent training scheme that ensures you get the skills you need.

I get to work with a lot of dedicated professionals with years of experience, and have picked up a lot from them. There's a really big team—not just the team in the vicinity, but also thousands of staff working for Capgemini across the world. We're all on a shared distribution list, so if you need an answer, there's someone in a different country, on a different account, who can provide you with an answer in a couple of minutes."

Bobby Spooner
Cybersecurity Consultant

An intern's view: My first steps into cybersecurity



I've always known I wanted to do something with computers, it was something I was always good at. I came into the Capgemini team with no practical experience. Everything I'd done in my two years at college prior to joining the program was entirely theoretical.

When I had my interview I was told that the role would not be completely technical, that there would be a mixture of everything. For instance, Capgemini sent me on a business writing course, which has taught me how to speak to people and compose emails—specifically to clients.

This has been a good mix of work, because I'm not the most technical person in the world. I don't want to just sit and code all day. The program has given me great insight into what the working world will be like at the end of my studies, and what I could potentially be doing for the rest of my life. In my third year at college I'm going to be doing a business module, and the experience I've gained here is definitely going to assist with that."

Alice Overton
Security Incident Investigator

come through, or are currently in, the graduate program.

The program takes on graduates, but also junior staff from across the business and interns still completing their college education. New starters get the support and protection from working with a large team, but also get the practical experience they crave to find out what they're good at, and what they're really interested in.

Most graduates entering the cybersecurity field are expected to have attained the skills they need in a 12-month program, but as the Capgemini program lasts for 24 months, these graduates spend more time working across an array of clients and industries, gaining valuable experience while enjoying a wide variety of challenges.

Mike verifies that Capgemini has hit on a winning retention formula with the program: "In five years, all but two of the graduates who have joined my team are still on board. In an industry known for struggling to hang on to talent, I think that says something."

WHERE CYBERSECURITY CONSULTANTS FIT IN

Putting together a robust internal cybersecurity team will ensure you have a cybersecurity resource that is closely aligned to the needs, processes, and objectives of your business. But as Mike rightly points out, there is a fair amount of expenditure and investment involved in finding, training, and retaining sufficient talent.

"It's not just the challenge of recruiting people—a lot of organizations can't afford to have a dedicated cybersecurity resource that they only utilize 25% of the time; it's a poor return on their investment. In a team like Capgemini's, however, we can make optimal use of all our people, and provide them with a diversity of projects and experience."

One way that Capgemini is approaching this is to create *Managed Security Operations Centers (SOCs)* to relieve the pressure on clients by outsourcing aspects of control, monitoring, and detection to a third party. An SOC also creates the ideal environment for bringing on new security talent. New starters can work alongside experienced consultants, getting involved early in live projects and enjoying the variety of work and challenges that keep them engaged.

Having a dedicated team from a partner like Capgemini means that organizations can also benefit a from "big picture" viewpoint of their risk areas, while their internal resources focus on upskilling and addressing on-the-ground minutiae.

"There's a balance," concurs Jérôme. "You need the deep tech knowledge, but you also need people who understand the business inside out. You need a combination of the right expertise at the right time."

No more is cybersecurity expertise a realm of deep-tech, cloak-and-dagger lone operators. Today's cybersecurity solution is more likely to comprise a combination of internal and external resources, senior consultants and junior monitors, business analysis and technical proficiency.

Whichever way businesses choose to structure their individual cybersecurity solution, both Jérôme and Mike agree that the next, most pressing challenge with regard to the cybersecurity skills gap is how to retain talent once it's been discovered.

"It's part of that personality type," explains Jérôme. "A good security expert is someone who is constantly curious, constantly learning… that means they also need to be constantly stimulated, constantly challenged."

"You need to have a passion to keep learning in this field," adds Mike. "Cybercriminals don't rest. Neither can we."

To learn more about the work that Capgemini's Cybersecurity experts are undertaking, see www.capgemini.com/secure-your-assets

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

About Capgemini and Sogeti

With more than 180,000 people in over 40 countries, Capgemini is a global leader in consulting, technology and outsourcing services. The Group reported 2015 global revenues of EUR 11.9 billion. Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Sogeti is a leading provider of technology and software testing, specializing in Application, Infrastructure and Engineering Services. Sogeti offers cutting-edge solutions around Testing, Business Intelligence & Analytics, Mobile, Cloud and Cybersecurity. Sogeti brings together more than 23,000 professionals in 15 countries and has a strong local presence in over 100 locations in Europe, USA and India. Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., listed on the Paris Stock Exchange.

Capgemini and Sogeti are experts in IT infrastructure and application integration. Together, we offer a complete range of cybersecurity services to guide and secure the digital transformation of companies and administrations. Our 2,500 professional employees support you in defining and implementing your cybersecurity strategies. We protect your IT, industrial systems, and the Internet of Things (IoT) products & systems. We have the resources to strengthen your defenses, optimize your investments and control your risks. They include our security experts (Infrastructures, Applications, Endpoints, Identity and Access Management), and our R&D team that specializes in malware analysis and forensics. We have ethical hackers, eight security operations centers (SOC) around the world, a Information Technology Security Evaluation Facility, and we are a global leader in the field of testing.

Find out more:

www.capgemini.com/secure-your-assets