WHY ADD SECURITY TO YOUR SKILL SET AND HOW TO DO IT!
4 Reasons Why Security Is Important to Practice in IT Roles

How Security Knowledge and Skills Enhance IT Careers

Steps to Moving Forward with Security
4 REASONS WHY SECURITY IS IMPORTANT TO PRACTICE IN IT ROLES

Your company’s data is everything. And today it is everyone’s job to safeguard it from breach. Whether you are already implementing security practices in your environment or not, the need to protect sensitive data — and the increasing skill of cyber criminals — means that every IT professional needs to take ownership of security.

Here are four reasons why you should be learning more about security and working closely with team members from the security department.
Security processes used to be seen as bottlenecks and barriers to innovation. That is not the case anymore. All corners of the organization are beginning to support security practices and know it needs to be baked into IT from the start of all initiatives. Thinking about the risk and compliance concerns of every project at the outset is one way to avoid a “no” response from the security folks once it is in development or well under way.

People with varying roles and responsibilities should be involved in security efforts. Building products and processes with risk in mind from the start requires collaborating with your security stakeholders to get their perspectives on day one. Find out how desired goals and outcomes might impact corporate risk posture.
Executive Management and the Board are Watching

Security is now everybody’s business in an organization. IDG research finds 44% of organizations have corporate boards that actively participate in their overall security strategy. The same research also finds 58% of boards are briefed on security at least quarterly.

With security obviously a high-level priority now in business, do you want to be left out of the action? Clearly risk is top of mind for those responsible for strategic priorities and the organization’s direction. To ignore this emphasis is bad for your career and bad for business.
YOU WANT TO KEEP YOUR NAME OUT OF THE HEADLINES

We’ve all seen some of the big brand names that have made their way to the headlines for all of the wrong reasons. This ties back to security as everyone’s business in an organization – particularly if one of the goals is to help the company stay out of the headlines because of a major data breach or incident.

A disconnect between security and other areas of IT can lead to security gaps. Without an understanding of how IT process and policies lead to vulnerabilities, the organization’s exposure to risk is high and it is only a matter of when – not if – a breach occurs.
THE INFOSEC SKILLS GAP WILL REQUIRE SECURITY KNOWLEDGE

The skills gap facing information security is severe and expected to grow. In fact, the cybersecurity skills crisis is predicted to leave up to 1.8 million jobs unfilled by 2022.

Companies are feeling the pinch and resorting to creative options to fill security roles. IT professionals of all backgrounds will need to learn more about and understand security and risk to offer value to their employers.

According to a report from (ISC)², “The dynamics of the gap—including the impact on businesses and individuals—are complex. Cybersecurity touches almost everyone in an organization. Employees from Legal to Marketing, Finance to Operations, are increasingly aware of how data flows through the organization and what it takes to keep it secure. Meanwhile, IT (IT/ICT) professionals are often responsible for securing their organization’s critical assets, but don’t have a formal information security title.”
TAKEAWAY: BUSINESS CONSIDERS SECURITY A PRIORITY – SHOULDN’T YOU?

As business leaders continue to ramp up investment in security priorities and allocate more budgetary dollars to risk mitigation, every IT professional should consider security part of their responsibility. The best way to position yourself as a valuable team player who understands security strategy is through education and training that will provide you with the skills you need.
Some estimates put the global cost of cybercrime at as much as $600 billion — about 0.8% of global GDP. Research from the Ponemon Institute finds the global average cost of a data breach is $3.86 million, a figure that rose 6.4% in 2018.

These numbers reveal the stark reality of the severe impact cybercrime has on the bottom line for business. Any organization that has not already made security a priority is going to find themselves hit with a breach or incident (if they have not been impacted already). And any IT professional who does not see the opportunity security presents for career development is failing to see the light.

But despite the numbers and opportunity, there are not nearly enough security pros entering the profession to meet the demand business has for security-skilled workers. Here are some compelling reasons to consider adding security knowledge and skills to further your IT career.
YOU WILL BE A HOT COMMODITY
As organizations struggle to fill infosec roles, those with security knowledge and skills will have their pick of positions. The nonprofit CyberSeek found that there were more than 300,000 cybersecurity job openings in the U.S. in 2018, a number expected to grow. CyberSeek also finds for every security job opening, only 2.5 qualified candidates exist. Clearly, having security training and education means job hunting odds will be in your favor.

SALARIES WILL BE HIGHER WITH SECURITY SKILLS
Because companies are pinched for infosec talent, they are paying high salaries to fill roles. The salary for an information security analyst was at $95,510 in 2017, according to the Bureau of Labor and Statistics – more than $10,000 above the $84,580 average for other computer-related positions.
YOU CAN CHART YOUR OWN CAREER COURSE
With security skills and training, companies will be eager to keep you satisfied and likely willing to let you chart a course for upward mobility and career development within the organization. That’s because in addition to hiring challenges, turnover is also high among security professionals due to great demand in the job market. Managers are often more than willing to accommodate their security-skilled staff’s requests for career development to keep them on the job for longer periods.

YOU WILL HAVE SKILLS YOU CAN USE FOR LIFE
Cybercriminals evolve and advance their skills annually, and the costs related to breaches and security incidents continue to climb. Demand for cybersecurity skills is increasing accordingly and shows no sign of slowing down.
EXCITING AND CHALLENGING SECURITY ROLES ARE CREATED ANNUALLY

Because of the unfortunate burgeoning skill set of cyber criminals, new career paths in security are also forming every year. For example, security professionals with an understanding of awareness are now helping corporations develop cyber awareness programs – a role that rarely existed a decade ago.
TAKEAWAY: WITH SECURITY, YOU’RE A HOT COMMODITY

The security career path is exciting and developing at a rapid pace. The skilled professional who has security training and education will continue to be in demand for many years to come.
The industry is struggling with a shortage of skilled professionals. Combine that with the constant game of cat and mouse business is forced to play with ever-industrious cybercriminals, and the outlook is good for challenging and rewarding work in your future. Here are some suggestions for moving forward.

1. **FIND A MENTOR**
   An experienced mentor can provide guidance on growing your career and building your personal brand. A mentor can also help you do a gut check when things are not moving along at the pace you would like, and offer perspective on what you might need to do to change course. Need ideas for finding a mentor? Attend meet-ups, conferences and other professional events for security professionals and get to know other attendees.

2. **GET TO KNOW INDUSTRY PLAYERS**
   Those meet-ups and conferences will also help you learn the names of influential thought leaders in the industry who are publishing research and doing innovative work in the field. The security industry is its own world, full of so-called “rock stars” and influencers that many admire. Even if you aren’t fully entrenched in a security role yet, attending events where you can get to know some of the industry influencers, and keeping up on security news online, will help you navigate the field with knowledge and confidence as you chart the course of your career.
3  BRUSH UP ON BASIC TECH
If you’re going to add security to your knowledge base, the most basic technical fundamentals should be understood in order to offer value to your organization. Not everyone in security comes from a deep technical background, but there are some essentials you need to dig when you’re getting started. At the very least, you need an understanding of systems, coding, networking, and how applications are run and maintained.

There are multiple ways to get this education, including books, online courses or even local community college classes, but these fundamentals will be essential as you get deeper into security work.

4  TRAIN AND EARN CERTIFICATIONS
Certifications give you more cred and show that you are passionate about education and staying on top of emerging industry trends. It shows current and potential employers that you are investing in the career and have specialized knowledge. In an ever-changing field, certifications help you stand out from generalists and can even give you a competitive edge over other job-seekers.
TAKEAWAY:
THERE’S NEVER BEEN A BETTER TIME TO ADD SECURITY TO YOUR SKILL SET

With security job openings at a record high, there has never been a more advantageous time to add cybersecurity to your role. Whether you are a tech generalist who is ready for a change, or a different kind of professional coming from a less technical background, the need for a wide variety of skills exists in many security positions. With passion, drive and flexibility, security-skilled professionals will find the opportunities to be plentiful well into the future.