Deloitte.

cyber 101

Cybersecurity Professionals Supplementary Reading

October 2017

Who are Cyber Professionals?

As long as headlines continue to report the crimes of cyber perpetrators against organisations, cyber security is not an optional choice and cyber security professionals are required.

Who are they?

Individuals responsible for protecting an organisation’s network, infrastructure and computer systems. Cybersecurity professionals have a broad range of skills beyond IT including an understanding in business process, vendor management, physical security, threat awareness, and business continuity management (not just disaster recovery).

3 Must Have Skills for Cybersecurity Professionals

1. A strategist to ensure protection of network, infrastructure and computer systems.

2. People management and communication skills to ensure effective coordination with teams and clients. He/she needs to communicate with every professional within an organization about the terms of IT.

3. Technical competency. One should always re-skills with advanced technology skills in order to be capable of grasping technical security issue immediate and resolve the same.

7 Cyber-Security Skills In High Demand

Businesses around the world report a shortage in cyber-security talent. Here are the skills IT managers should be seeking to keep their data secure.

“An asset is what we’re trying to protect”

Asset – People, property, and information.

http://www.disaster-resource.com/index.php?option=com_content&view=article&id=1717:the-importance-of-cyber-security-within-your-organization
https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article
https://www.darkreading.com/careers-and-people/health-it-and-cybersecurity-5-hiring-misconceptions-to-avoid/a/d-id/1329932?

Roles and Responsibilities

The myriad advanced threat vectors and emerging technologies require cybersecurity professionals to be skilled in technology as well as business and communications.

Typical responsibilities of cyber security professionals include:

Developing and designing security architecture (devices and software) to ensure safety of client's information.

Managing security measures and performance of information technology system within an organization's network.

Operating regular inspections of system and network processes for security updates and potential breaches.

Conducting audit process for initiating security and safety measures and strategies.

Customizing access to information as per identity and necessity.

Maintaining and improving information security policy, procedure, services and standards.

The Importance Of Cyber Security Within Your Organization

Information Availability & Security

Written by Ted Brown

You know that Cyber Security is an important Business Continuity Planning (BCP)/COOP issue, but like everything else in the BCP/COOP world, unless you get buy-in across the board, Cyber Security policies and procedures will be ignored.

So the purpose of this article is to prepare you to articulate the importance of Cyber Security, to gain allies to implement procedures, and to justify the value of a Cyber Security Audit. After all, Cyber Security concerns more than the Information Technology (IT) and BCP/COOP departments.

As the world becomes increasingly interconnected, Business Continuity/COOP professionals must pay more attention to the security of their organization's connections. It seems like every week there are new headlines about hackers bringing an organization to its knees. The stolen funds, bad publicity, and

https://www.darkreading.com/application-security/the-team-of-teams-model-for-cybersecurity/a/d-id/1329840?
https://www.simplilearn.com/it-security-professionals-key-roles-responsibilities-article
https://monstercloud.com/importance-of-cybersecurity/

"A threat is what we're trying to protect against."

Threat – Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.

Why is there a shortage?

There are no signs of the bad guys limiting their talent pools and cybercrime is now a US$445 billion industry with a trajectory of possibly trillions.

To illustrate, toolkits developed by cyber criminals have adapted cloud and managed service business models to propagate and expand cyber criminal activities. These toolkits are easily obtainable with no formal education required to learn how to use them. The revenue from the sales of these toolkits go on to fund more elaborate schemes designed to create chaos and opportunities to rob organisations of their assets.

Cybercriminals are becoming more organised and aggressive while the good guys are struggling to fill their ranks.

In short, the frequency of successfully executed cybercrimes as a result of current day open network society, coupled with the use of cloud services and applications, have created an urgent need in organisations to rapidly advance their cybersecurity countermeasures.

Cybersecurity experts who possess the knowledge, education and most importantly, the thought process necessary to confront the difficulties that accompany the constantly evolving cyber activities are in demand to tackle the challenges posed in the cyber world.

20 Interview Questions and Answers for Cyber-security Professionals

Scott Barman

Last updated September 19, 2017

75604 Views 1 Comment

"A vulnerability is a weakness or gap in our protection efforts."

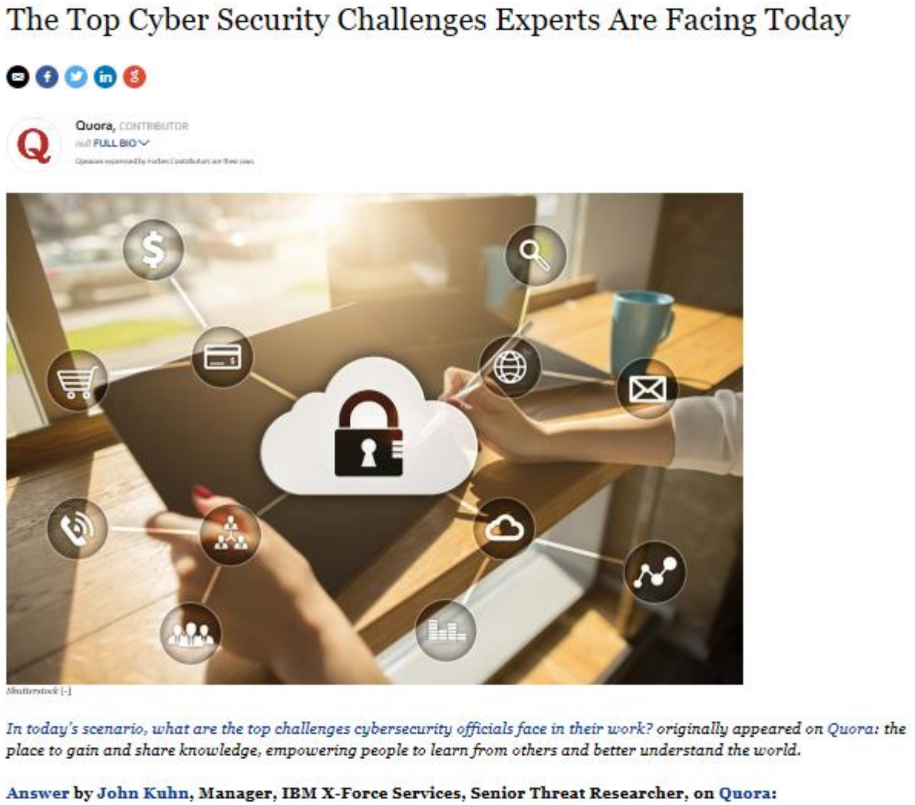
Vulnerability – Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

https://www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/
https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it
https://monstercloud.com/importance-of-cybersecurity/

More facts on the shortage of cyber professionals

Reason:

- Formal education, professional certification and training are required to become a cyber security professional
- As the rise of cyber attacks escalate, schools are not graduating enough cyber security professionals to keep up with the ongoing cyber attacks
- Recent research by Cisco showed that 29% of breached organisations lost revenue and according to the World Economic Forum’s Global Risks Report
- Most organisations face challenges in interpreting the detection or mitigation of cyber security threats



The Top Cyber Security Challenges Experts Are Facing Today

Quora, CONTRIBUTOR
FULL BIO
Opinions expressed by Forbes Contributors are their own.

Shutterstock [-]

In today’s scenario, what are the top challenges cybersecurity officials face in their work? originally appeared on Quora: the place to gain and share knowledge, empowering people to learn from others and better understand the world.

Answer by John Kuhn, Manager, IBM X-Force Services, Senior Threat Researcher, on Quora:

“A vulnerability is a weakness or gap in our protection efforts.”

Vulnerability – Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.

https://www.forbes.com/sites/quora/2017/05/31/the-top-cyber-security-challenges-experts-are-facing-today/#4b266dda2238
https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/#7f2f1edd5163

What can you do?

Here are some suggestions on what organisations can do to address the shortage of cyber security professionals

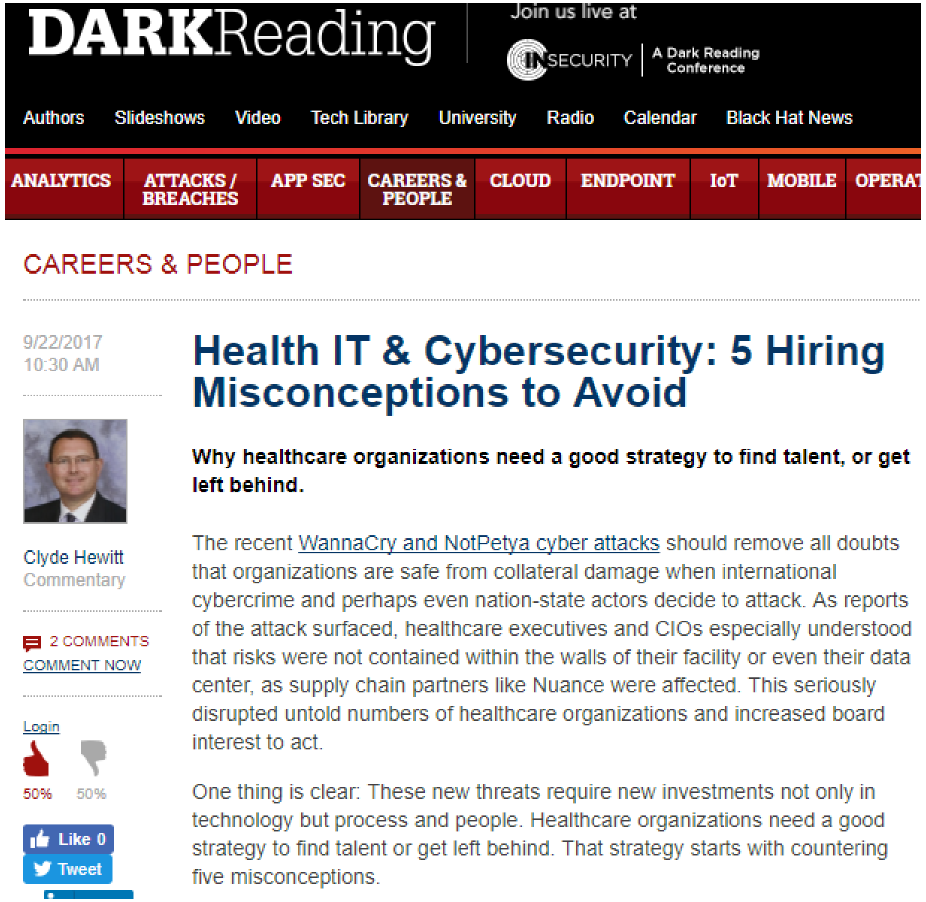
Re-examine your workforce strategy by recognizing the qualities required to run a successful security program and expand hiring efforts beyond career fairs to include polytechnics, local universities and any other avenues.

Have a robust support program for new hires such as mentorships, rotational assignments and shadowing to help new cybersecurity hires to gain visibility and experience. Keeping new hires engaged by giving them the freedom to work on different projects allows them to apprehend new technologies and services.

Build a local cybersecurity ecosystem by connecting with government organisations, educational institutions and other groups to explore and generate interest in the cybersecurity field.

With cybersecurity being a highly dynamic field, continuous learning and upskilling are required to **develop a strong culture of risk awareness**.

Cybersecurity is a complex career field with extraordinarily challenging problems, but with a diverse pool of experiences and ideas, we stand a much better chance of successfully defending our assets.



CAREERS & PEOPLE

9/22/2017
10:30 AM

Clyde Hewitt
Commentary

Health IT & Cybersecurity: 5 Hiring Misconceptions to Avoid

Why healthcare organizations need a good strategy to find talent, or get left behind.

The recent WannaCry and NotPetya cyber attacks should remove all doubts that organizations are safe from collateral damage when international cybercrime and perhaps even nation-state actors decide to attack. As reports of the attack surfaced, healthcare executives and CIOs especially understood that risks were not contained within the walls of their facility or even their data center, as supply chain partners like Nuance were affected. This seriously disrupted untold numbers of healthcare organizations and increased board interest to act.

One thing is clear: These new threats require new investments not only in technology but process and people. Healthcare organizations need a good strategy to find talent or get left behind. That strategy starts with countering five misconceptions.

https://www.darkreading.com/careers-and-people/health-it-and-cybersecurity-5-hiring-misconceptions-to-avoid/a/d-id/1329932?
https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it

"Risk is the intersection of assets, threats, and vulnerabilities."

Risk – The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Deloitte.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.