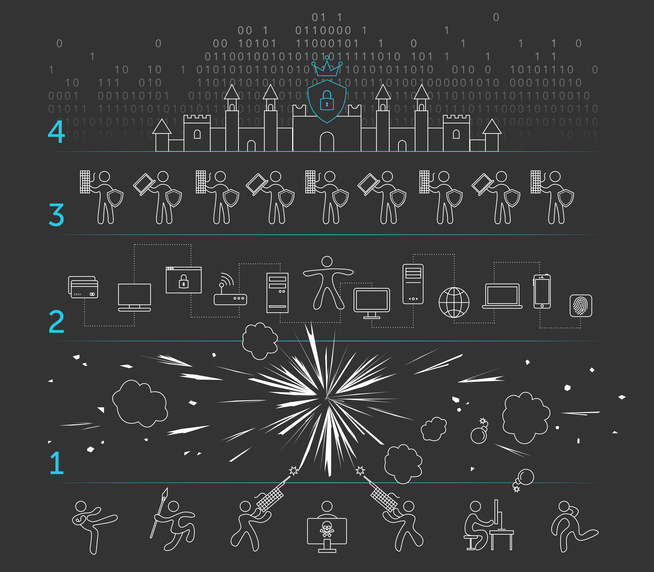
SECURING QUALIFIED TALENT IN THE EVOLVING FIELD OF CYBERSECURITY

TRILOGY
EDUCATION SERVICES

A shortage of cybersecurity professionals has affected both the public and private sectors for years. That shortage is becoming more acute as the demand for qualified talent increases rapidly. As cyber-criminals continue to tarnish brands by exposing their vulnerabilities, companies must secure their data by securing a workforce that can stop these threats in their tracks.



1. FAMOUS BREACHES

Especially in recent years, the need for cybersecurity expertise has been highlighted by a string of high-profile data breaches.

2017 — verizon

Caused by a misconfigured security setting on a cloud server, the Verizon breach led to the personal data of 6 million customers–including phone numbers, names, and some PIN codes–becoming publicly available online.

2017 — EQUIFAX

The Equifax breach exposed the personal information of 143 million consumers, including Social Security Numbers, dates of birth, addresses and, in some cases, driver's license numbers. Additionally, 209,000 consumers had credit card data exposed. The breach was estimated to have begun in mid-May, but was not discovered until July 29.

2016 — UBER

The Uber breach resulted in the personal information of 57 million users and 600,000 drivers being exposed. Hackers were able to access Uber's GitHub account, where they found username and password credentials to Uber's AWS account.

2014 — HOME DEPOT

When the company's POS system became infected with malware that posed as anti-virus software, the theft of credit and debit card information of 56 million customers occured. The company estimated $161 million of pre-tax expenses for the breach, including a consumer settlement and expected insurance payouts.

2013 – 2014 — YAHOO!

Yahoo announced that data associated with at least 500 million accounts had been stolen. Three months later, Yahoo disclosed a second breach affecting more than one billion accounts. The attack compromised users' names, email addresses, dates of birth, and telephone numbers. The Yahoo breach was not revealed until 2016. Later, the company revealed that another breach by a different group of hackers had compromised 1 billion accounts, which they later revised 3 billion accounts.

2013 — TARGET

During the holiday shopping season, approximately 40 million Target customers had credit and debit card information stolen. Target later paid $10 million to customers who were victims of the breach and tens of millions more to U.S. banks that had to reimburse customers.

2012 — LinkedIn

More than 100 million LinkedIn members were affected when a hacker breached the networking site and attempted to sell the account information online. This breach was not exposed until four years after it took place.

2. CYBERSECURITY IS NO LONGER AN AFTERTHOUGHT. IT'S NECESSARY TO A COMPANY'S SURVIVAL (AND REPUTATION)

$6 Trillion

The global cybercrime epidemic is predicted to cost the world $6 trillion annually by 2021 (up from $3 trillion per year in 2015).

Paying out expensive settlements is the most basic repercussion companies face after falling victim to a cybersecurity breach. Although news outlets cover the direct cost associated with such breaches, the impact on a company's value cannot be understand.

79%

According to PwC's 2015 State of US Cybercrime Survey, a record 79% of survey respondents (500 US executives, security experts, and others from the public and private sectors) said they detected a security incident in the past 12 months.

14.8%

Over the long term, the share prices of breached companies do continue to rise, but at a much slower pace. A study by Comparitech of 24 companies that experienced breaches saw a 45.6% increase in share price during three years prior to breach, and only 14.8% growth in the three years after.

40%

Breached companies typically underperform the NASDAQ. On average, they recover to the index's performance level after 38 days, but after three years, the NASDAQ ultimately outperforms them by a margin of over 40 percent.

31%

According to a 2017 Ponemon research study, breached companies, 31% of consumers impacted by a breach stated that they discontinued their relationship with the affected brand.

3. COMPANIES NEED TO HIRE THE NECESSARY TALENT TO PROTECT BOTH THEIR CUSTOMERS AND BUSINESSES

$170 Billion

By 2020, companies' investments in cybersecurity are expected to grow to $170 billion (up from $75 billion in 2015)

350,000

In 2017, the U.S. employed nearly 780,000 people in cybersecurity positions. That same year, in the U.S., 350,000 cybersecurity job positions were open.

65%

Approximately 65% of large U.S. companies have a CISO (Chief Information Security Officer) position, up from 50 percent in 2016.

100%

Cybersecurity Ventures predicts that 100 percent of large companies globally will have a CISO position by 2021.

61%

Cybersecurity leaders are in such high demand that 61 percent of C- and VP-level professionals are solicited to consider other cybersecurity jobs by various types of recruiters at least once per week.

45%

According to research from early 2017, 45% of organizations claim to have a problematic shortage of cybersecurity skills.

9%

Cybersecurity professionals command an average salary premium of nearly $6,500 per year, or 9%, more than other IT workers.

36%

U.S. News and World Report ranked a career in information security analysis 8th on its list of the 100 best jobs for 2015, stating the profession is expected to grow at a rate of 36.5% between 2012 and 2022.

4. TOP SKILLS YOU NEED FOR A CYBERSECURITY CAREER

As intrusion techniques evolve, so too will the skills that cybersecurity experts need in order to thwart them. Needed skills include:

Wireshark	Packet and protocol analysis	Familiarity with TCP/IP, HTTP, and other protocols
Tapping into networks	Network monitoring	Packet analysis
Threat intelligence	Database management	Machine learning
HTTP	JavaScript	SQL
XSS	XSRF	Familiarity with cookie-based authentication
John the Ripper (JTR)	Hashing algorithms	Password storage best practices
Dictionary attacks	Brute-force attacks	Metasploit
Kali Linux	Vulnerability Management Solutions / Vulnerability Scanners	Network intrusion
Python	Digital forensics	Electronic discovery
Data recovery	Encryption and decryption	

Training providers must maintain relevant curricula that are aligned to job needs, while students must seek out market-driven programs that adapt quickly to changing needs in order to best prepare graduates with the necessary skills.

SOURCES

http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html
http://money.cnn.com/2017/07/21/technology/verizon-data-leaked-online/index.html?iid=EL
https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html
https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#1c712a932fea
https://www.csoonline.com/article/3210347/it-careers/cybersecurity-job-market-statistics.html
http://sandhill.com/article/top-five-it-security-salaries/
https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
https://www.switchup.org/blog/high-demand-tech-jobs-in-2017-1-cybersecurity
http://burning-glass.com/research/cybersecurity/
http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/2015-us-cybercrime-survey.pdf
https://fortune.com/2017/09/11/equifax-stock-cybersecurity-breach/
https://www.scmagazine.com/study-finds-breach-companies-underperform-nasdaq/article/674304/
https://www.comparitech.com/blog/information-security/data-breach-share-price/
http://www.computerweekly.com/opinion/The-true-impact-of-a-cyber-breach-on-share-price
https://www.helpnetsecurity.com/2017/05/16/data-breach-stock-price/
https://www.csoonline.com/article/3238765/security/cybersecurity-skills-shortage-creating-recruitment-chaos.html

TRILOGY
EDUCATION SERVICES

ABOUT TRILOGY EDUCATION SERVICES

Trilogy is a workforce accelerator that empowers the world's leading universities to prepare professionals for high-growth careers in the digital economy. From full-stack development to data analytics, the company creates and manages skills-based training programs that are university-run, student-tested, and employer-approved. Since launching in 2015, Trilogy has enabled universities to transform the lives of thousands of program graduates with the technical skills to meet the needs of regional employers and the confidence needed to succeed in their careers. Learn more at www.trilogyed.com