Persistent challenges facing global cybersecurity leaders

George Do
CISO @Gojek and GoTo Financial

A bit about myself..

Current

- CISO @ Gojek & GoTo Financial

Prior

- Chief Information Security Officer @ Equinix
- Director of Information Security @ Tivo Inc
- Security Architect @ Exodus / Savvis Communications
- Security Engineer @ NASA

Security truths

- **Assume you are breached already**
- **Stress, anxiety and burnout come with the job**
- **It takes only one user or incident to ruin everything**

Challenge accepted?

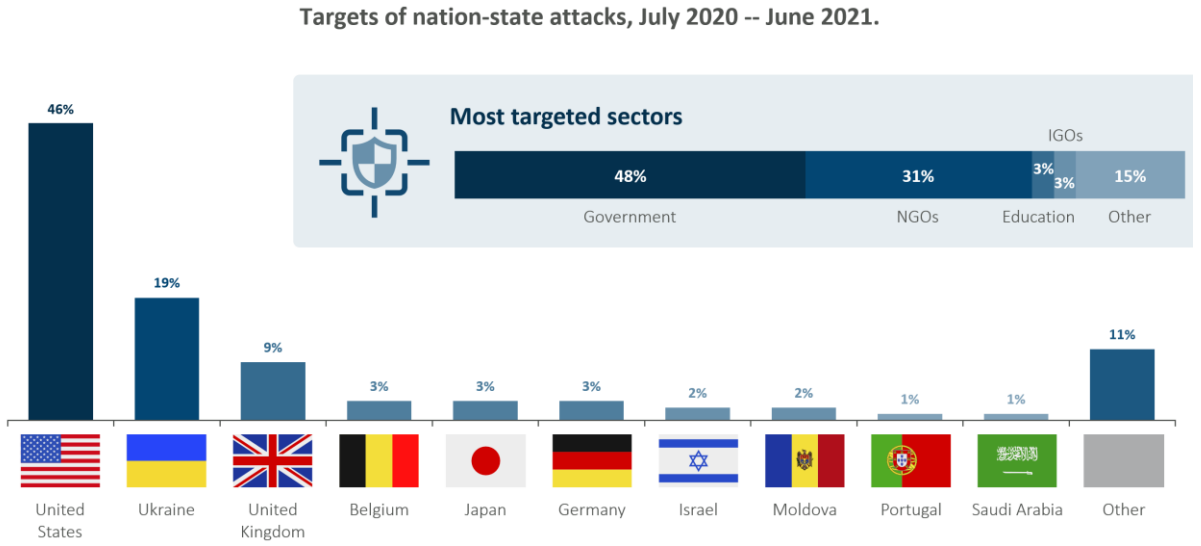
Challenge 1: Data breaches can come from anywhere

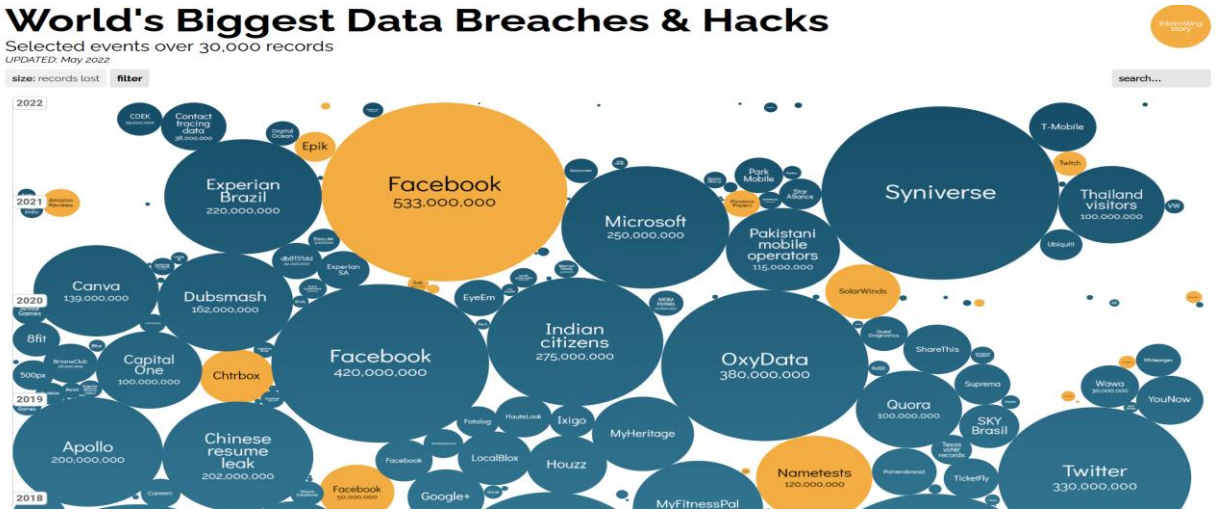
Challenges

- Cyber threats coming from all sides
- Threats constantly evolve
- Cyber risks cannot be reduced to zero

How we address

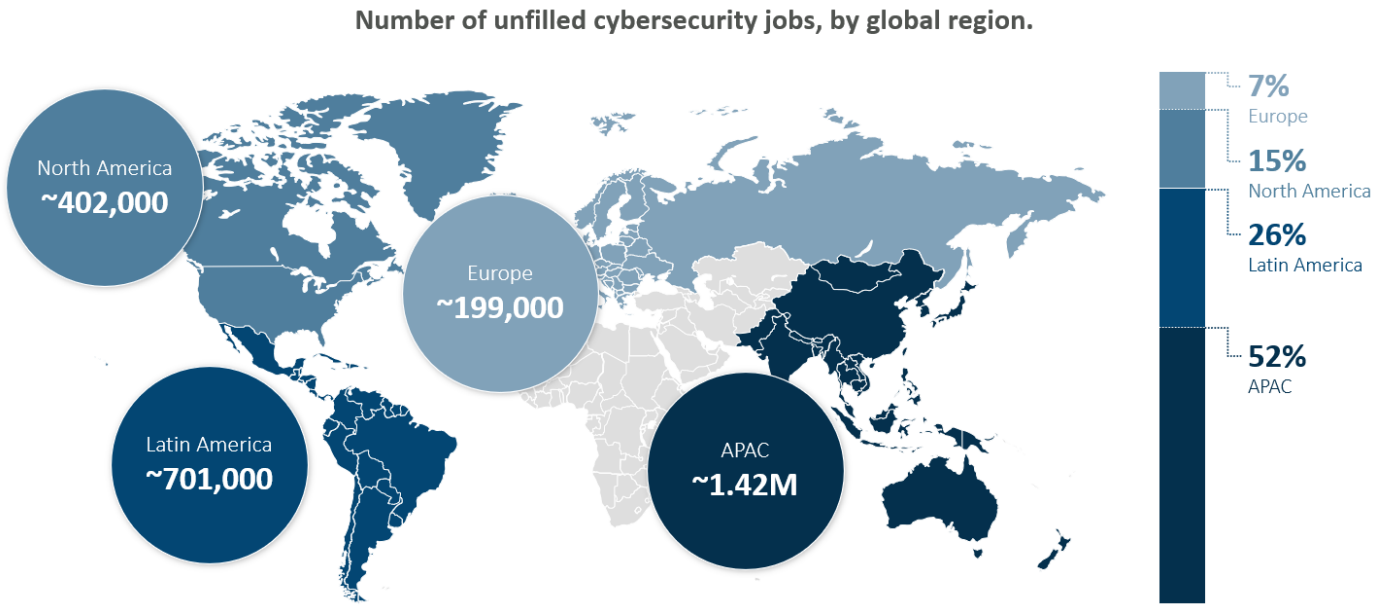
- Robust cybersecurity program
- Defenders must band together
- Intelligence sharing





Source: Microsoft, "Digital Defense Report," October 2021
Source: https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Challenge 2: Addressing the cybersecurity skills gap



Challenges

- We are recruiting from the same talent pool
- Shortage of talent = higher costs
- Demand is/will be much higher than supply

How we address

- Promote cybersecurity curriculum and programs at high school / universities
- Infosec champions programs / recruit internally
- Hackathons

Source: ISC2 Cybersecurity Workforce Study, Oct. 2021

Challenge 3: Securing the human

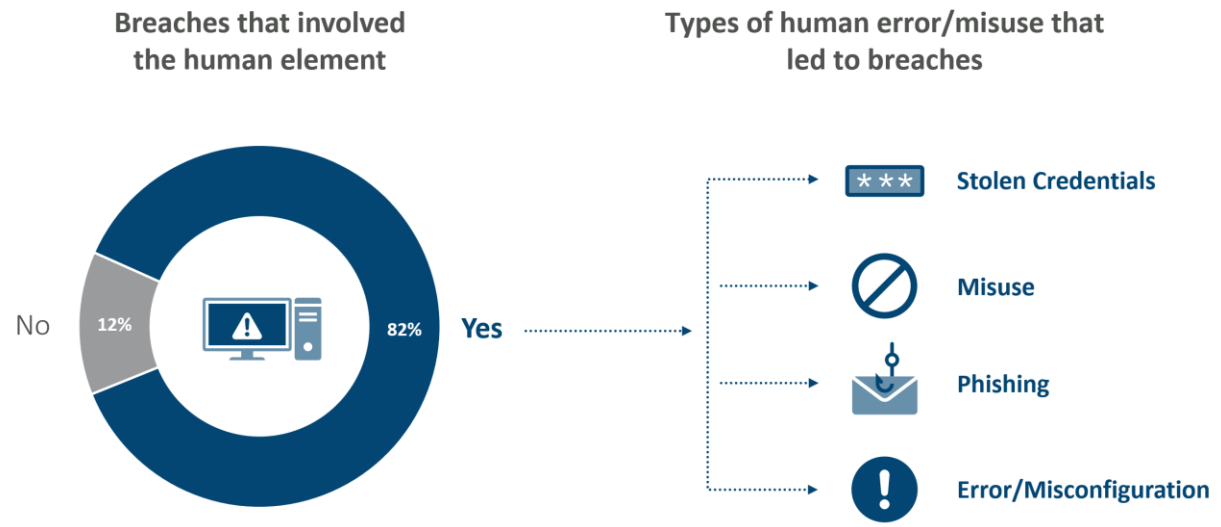
Challenges

- Users coming and going all the time
- Lots of applications; lots of devices
- Data is everywhere

How we address

- Endpoint security
- Security awareness training
- Phishing campaigns
- Internal bug bounty program
- Hackathons
- Data loss prevention
- …

82% of 2021 Data Breaches Involved Human Error/Misuse



Source: Verizon, 2022 Data Breach Investigation Report, May 2022

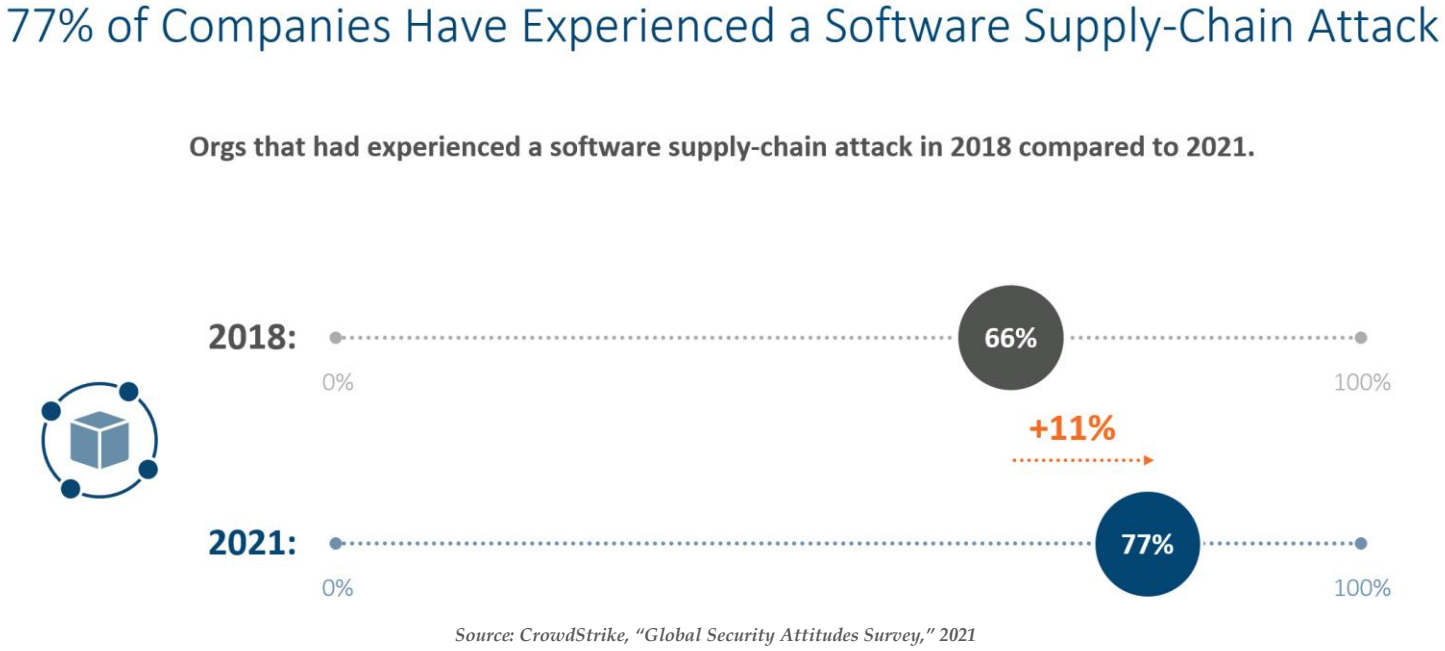
Challenge 4: Rising 3rd party risks

Challenges

- Data has left our premise / we no longer have control
- 3rd parties have weak security
- Commonly overlooked / high impact

How we address

- 3rd party risk assessments
- Vendor checklists
- Qualifying with SecurityScorecard and other tools
- Contractual liabilities for breaches



Source: CrowdStrike, "Global Security Attitudes Survey," 2021

Roles that cybersecurity leaders must embrace

- **Salesman – you are selling security everyday**
- **Strategist / Architect – optimizing security across tech stacks and processes**
- **Auditor – constantly measuring, reporting and remediating gaps**
- **Engineer – deploy and operate security solutions**
- **Project manager – ensure security projects and initiatives are executed**
- **Lawyer – advising the board, executive team and key stakeholders on cyber**
- **…**

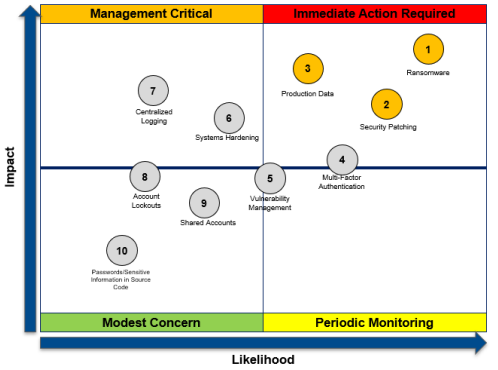
Tips for success

- **Align security to the business**
  - Quantify cybersecurity risks to business impact
  - If you cannot measure it, it has no impact

Chief Executive Officer	Chief Financial Officer	Chief Legal Officer	Information Technology	Engineering
CISO	CISO	CISO	CISO	CISO
Information Security				

- **Reporting to the board; skills required**
  - Quantify security risks in business terms
  - Business impact is critical

Security Risk Register		
Rank	**Risk**	**Status**
1	**Ransomware** attacks lead security breaches, financial fraud, loss of sensitive data, and brand damage (impact to shareholder value)	
2	Lack of **Security Patching** on technology systems leaves our infrastructure highly susceptible to cyber attacks and data breaches	
3	Use of **Production Data in Development** environments leaves critical data at risk of compromise due to lower security environments in non-Dev	
4	No **Multi-Factor Authentication** leaves applications and systems vulnerable to unauthorized access	
5	**Vulnerability Management** – lack of ongoing tracking and remediation of vulnerabilities on systems make them easier to attack and compromise	
6	**Systems Hardening** – lack of ongoing security re-configuration of systems to acceptable security standards leaves it open to hacking	
7	**Centralized Logging** – not logging to a central location results provides no audit trails and breach and threat alert on systems	
8	Lack of consistent **Account Lockouts** policy enforcement allows for brute force attack making it easier for systems to be breached	
9	Use of **Shared Accounts** allows bad actors to gain access to many systems by compromising just one user account with no audit trails	
10	Inclusion of **Secrets in Source Code** gives instant system access to applications and systems to attackers	



- **Pair accountability and empowerment**
  - Define security reporting structures and budgets
  - What is the security team is “NOT” responsible for

George Do
CISO @Gojek and GoTo Financial