bâton | global

HOW TO GET EXECUTIVES TO BUY INTO YOUR SECURITY PLANS

OCT 6TH 2021 | SECURE IOWA

INTRODUCTION

WADE BRITT, MIBS

Chief Operating Officer

Wade is an experienced P&L leader with a track record of driving change, performance improvement, and margin enhancement with B|G since 2016.

15 years logistics sector experience in Europe, South Asia and the US.

10 years ed tech sector in the US, South America and India.

He earned a Masters of International Business Studies and a Bachelor of Arts from the University of South Carolina.

Bâton Global

Bâton Global (B|G) is driven by a desire to bring together the best of academic research with cutting-edge technologies and leading global business experience.

Our mission is to provide strategy, innovation, leadership and research services for solving our clients' most complex challenges, transforming organizations and communities worldwide.

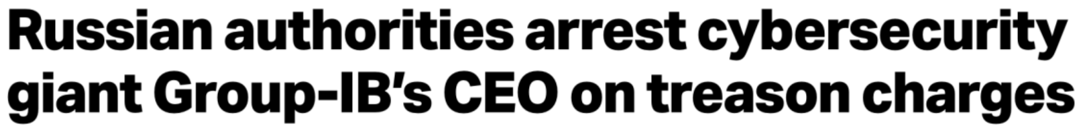
CHALLENGES OF GETTING BUY-IN

- Lack of understanding of potential impact
- Inability to quantify impacts for your firm
- “Red Ocean” budget environment

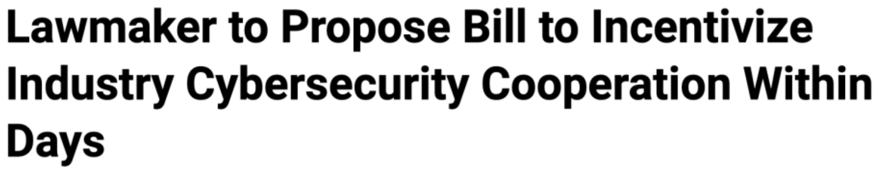
- Wishful thinking
- Risk aversion
- Turf protection

ATTACKS UP 29% H1 2021

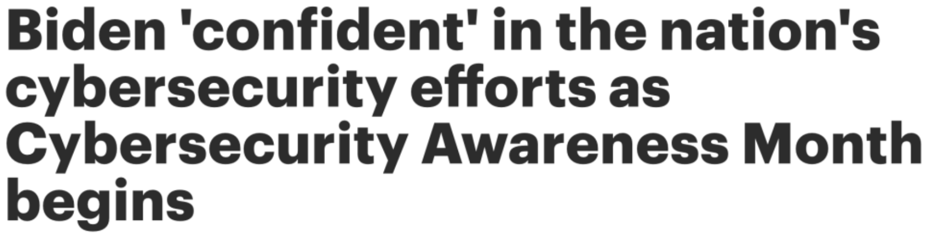
Ransomware attacks surge 93%



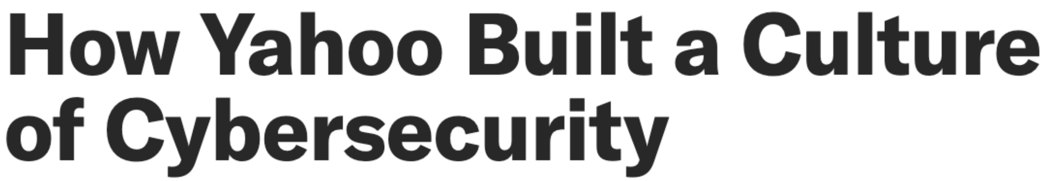
Russian authorities arrest cybersecurity giant Group-IB’s CEO on treason charges



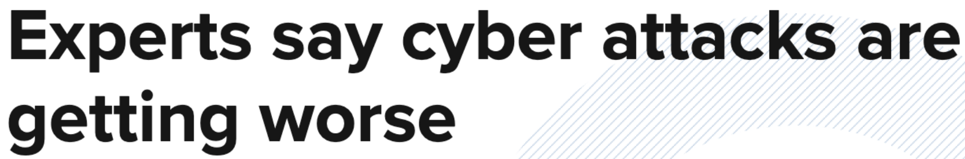
Lawmaker to Propose Bill to Incentivize Industry Cybersecurity Cooperation Within Days



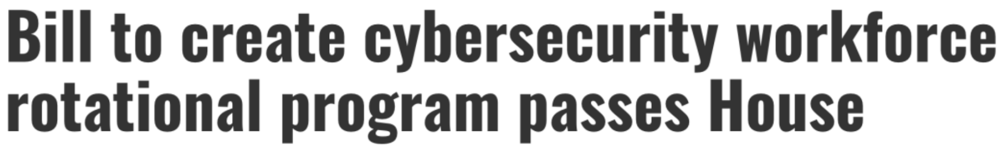
Biden 'confident' in the nation's cybersecurity efforts as Cybersecurity Awareness Month begins



How Yahoo Built a Culture of Cybersecurity



Experts say cyber attacks are getting worse



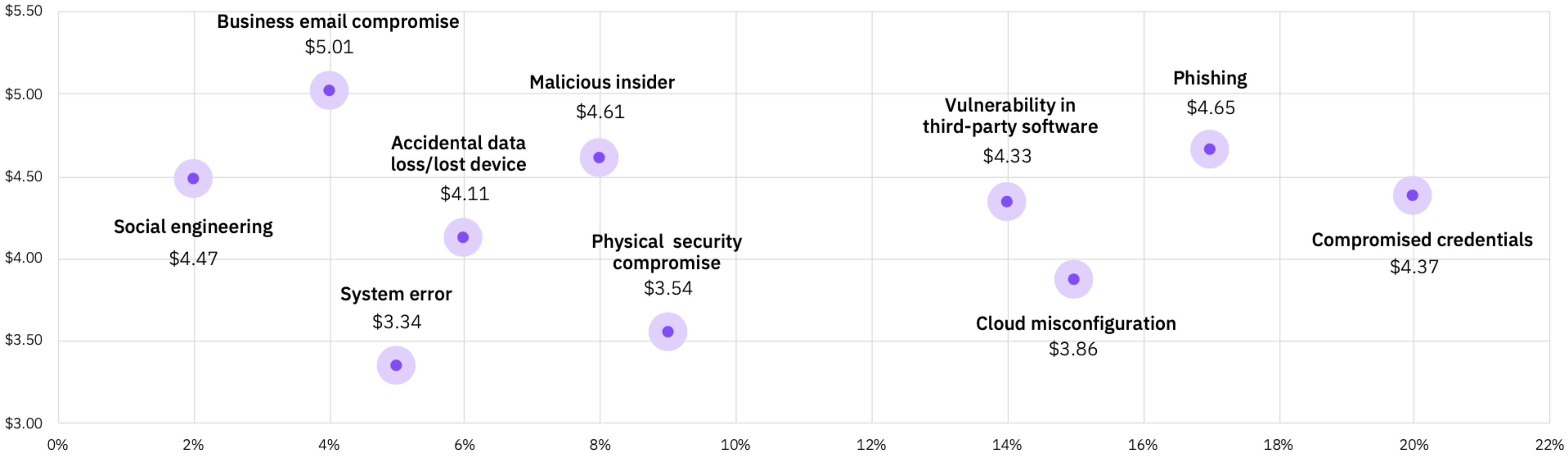
Bill to create cybersecurity workforce rotational program passes House

KEY EVENTS IN 2021

- **AUGUST** | Howard University canceled classes following a hack of their systems, which is representative of a rise in ransomware attacks on education providers in the U.S.
- **JULY** | The IT firm Kaseya was hacked, resulting in thousands of victims in at least 17 countries getting locked out of their systems. The hackers initially requested a total of $70 million in ransom.
- **JUNE** | An attack on the multi-national meat manufacturer JBS S.A. closed off a quarter of American beef operations for two days, as the firm shut down its computer systems to limit the scale of the breach. The same group, REvil, hacked both JBS and Kaseya.
- **MAY** | A cyberattack on Colonial Pipeline forced the company to shut off gasoline supply to much of the Eastern Seaboard, resulting in shortages throughout the South. That same month, an attack shut down the databases of a hospital system in San Diego for two weeks.
- **APRIL** | Hackers claimed to have stolen 500 gigabytes of data from the Houston Rockets, including contracts and non-disclosure agreements.
- **MARCH** | CNA Financial Corp, one of the largest insurance companies in the U.S., was locked out of their network for almost two weeks following a breach.
- **FEBRUARY** | Hackers accessed a water-treatment plant in Oldsmar, Florida, briefly raising the lye in drinking water to dangerous levels.

These are some of the most damaging break-ins, but they are far from the only examples: **One security firm that tracks ransomware attacks estimated that there were some 65,000 successful breaches in 2020.**

ATTACK VECTORS



DETECTION AND ESCALATION

Activities that enable a company to reasonably detect the breach.

- Forensic and investigative activities
- Assessment and audit services
- Crisis management
- Communications to executives and boards

LOST BUSINESS

Activities that attempt to minimize the loss of customers, business disruption and revenue losses.

- Business disruption and revenue losses from system downtime
- Cost of lost customers and acquiring new customers
- Reputation losses and diminished goodwill

NOTIFICATION

Activities that enable the company to notify data subjects, data protection regulators and other third parties.

- Emails, letters, outbound calls or general notice to data subjects
- Determination of regulatory requirements
- Communication with regulators
- Engagement of outside experts

POST BREACH RESPONSE

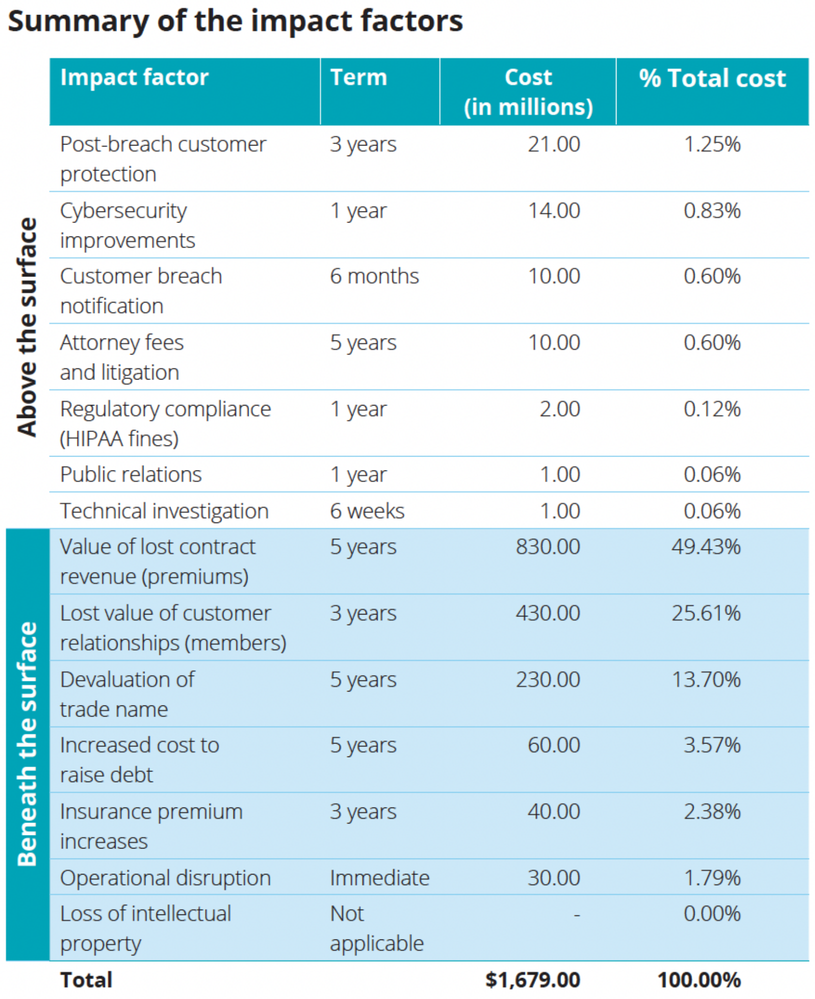
Activities to help victims of a breach communicate with the company and redress activities to victims and regulators.

- Help desk and inbound communications
- Credit monitoring and identity protection services
- Issuing new accounts or credit cards
- Legal expenditures
- Product discounts
- Regulatory fine

COST IMPACTS

A quantitative risk assessment of cyber security can be applied to your business:

- Healthcare case study places cost impact at 2.8% of revenue
- Tech manufacturing case study places cost impact at 8% of revenue
- A basic model for your firm could apply the proportions from the case study using your annual revenue and a worst-average-best case calculation
- Smaller firms are likely to have disproportionately higher impacts



Summary of the impact factors

	Impact factor	Term	Cost (in millions)	% Total cost
Above the surface	Post-breach customer protection	3 years	21.00	1.25%
	Cybersecurity improvements	1 year	14.00	0.83%
	Customer breach notification	6 months	10.00	0.60%
	Attorney fees and litigation	5 years	10.00	0.60%
	Regulatory compliance (HIPAA fines)	1 year	2.00	0.12%
	Public relations	1 year	1.00	0.06%
	Technical investigation	6 weeks	1.00	0.06%
Beneath the surface	Value of lost contract revenue (premiums)	5 years	830.00	49.43%
	Lost value of customer relationships (members)	3 years	430.00	25.61%
	Devaluation of trade name	5 years	230.00	13.70%
	Increased cost to raise debt	5 years	60.00	3.57%
	Insurance premium increases	3 years	40.00	2.38%
	Operational disruption	Immediate	30.00	1.79%
	Loss of intellectual property	Not applicable	-	0.00%
	Total		**$1,679.00**	**100.00%**

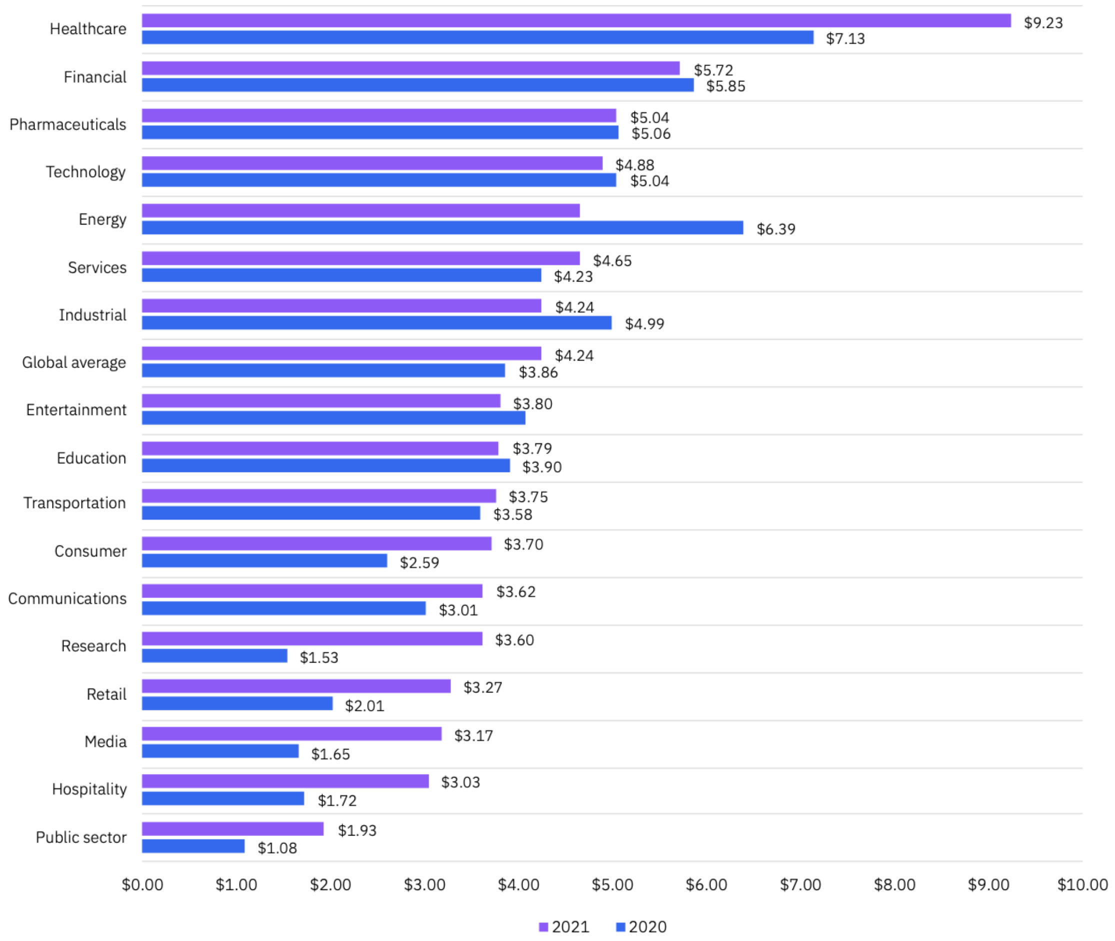
COST IMPACTS

Key impact KPIs:

- Average cost of a ransomware attack: $4.62m
- Average cost of a data breach attack: $4.24m
- Average cost of breach caused by email compromise: $5.01m
- PII per record cost: $180
- 10% increase in cost impact from 2020-2021
- -7.27% decrease in share price with estimated 1.8% decline that never recovers

Average total cost of a data breach by industry

Measured in US$ millions



CENTERS OF INFLUENCE

🧠

- CFO/Finance organization
- Business case led
- “Above the line” focused – tangible impacts that can be quantified

🫀

- CRO/CMO organizations
- Reputational and revenue impact led
- “Below the line” focused – softer but scarier

WHERE DO I GET STARTED?

- Don’t eat the elephant in one bite
- Map areas of highest risk and focus accordingly
- Key activities:
    - Information security risk assessment
    - Business continuity
    - Vulnerability scan
    - Penetration test
    - Social engineering test

REFERENCES

SLIDE 8 – COST IMPACTS | BENEATH THE SURFACE OF A CYBERATTACK: A DEEPER LOOK AT BUSINESS IMPACTS | Deloitte | https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html

SLIDE 6 - ATTACK VECTORS | SLIDE 9 – COST IMPACTS | COST OF A DATA BREACH REPORT 2021 | IBM | https://www.ibm.com/security/data-breach

SLIDE 9 – COST IMPACTS | THE IMPACT OF CYBER BREACH ON COMPANY MARKET VALUATION | David Shrier | https://esmelearning.com/blogs/news/the-impact-of-cyber-breach-on-company-market-valuation

ALTERNATIVE RISK RATING CALCULATIONS | CYBER VALUE AT RISK: QUANTIFY THE FINANCIAL IMPACT OF CYBER RISK | Bay Dynamics | https://www.ten-inc.com/presentations/2017_ISE_NE_BayDynamics_WP.pdf

SLIDE 4 – HEADLINE | 2021 Cyber Attach Trends MID-YEAR REPORT | Check Point | ·https://pages.checkpoint.com/cyber-attack-2021-trends.html

WHAT'S DRIVING THE SURGE IN RANSOMWARE ATTACKS? | Matt Stieb | https://nymag.com/intelligencer/article/ransomware-attacks-2021.html

SIGNIFICANT CYBER INCIDENTS SINCE 2006 | Center for Strategic and International Studies (CSIS) | Washington, D.C.

LIST OF DATA BREACHES AND CYBER ATTACKS IN AUGUST 2021 – 61 MILLION RECORDS BREACHED | ITGovernance.co.uk | https://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-august-2021-61-million-records-breached

Q&A

bâton | global

bâton global