



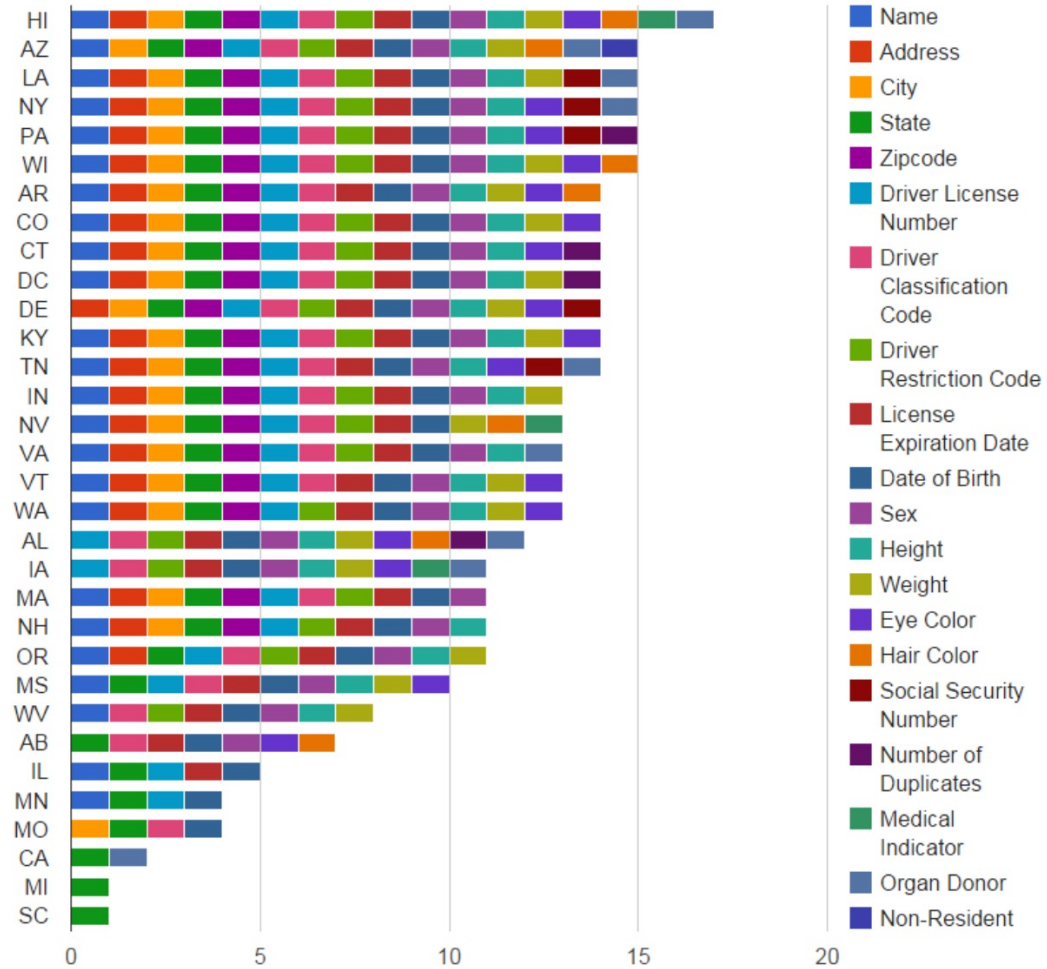
To Trust of Not To Trust

What Every Startup Needs To Know About Privacy and Cybersecurity

CONNECTS Seminar at Carnegie Mellon: January 21, 2025

John Funge, DataTribe

Drivers License Attributes on 2D Barcode by State



Source: <http://mantascodes.com/us-drivers-license-barcode-attributes-by-state/>

“Mark Zuckerberg declared in 2010 that privacy is no longer a “social norm,” but bought the four houses abutting his Palo Alto home to help ensure his own privacy.”

Schneier, Bruce. *Data and Goliath*

“I believe there's an opportunity to set a new standard for private communication platforms...”

Mark Zuckerberg, *A Privacy-focused Vision for Social Media*, March 2019





Major Cyber Incidents Over Time

Major cyber incidents

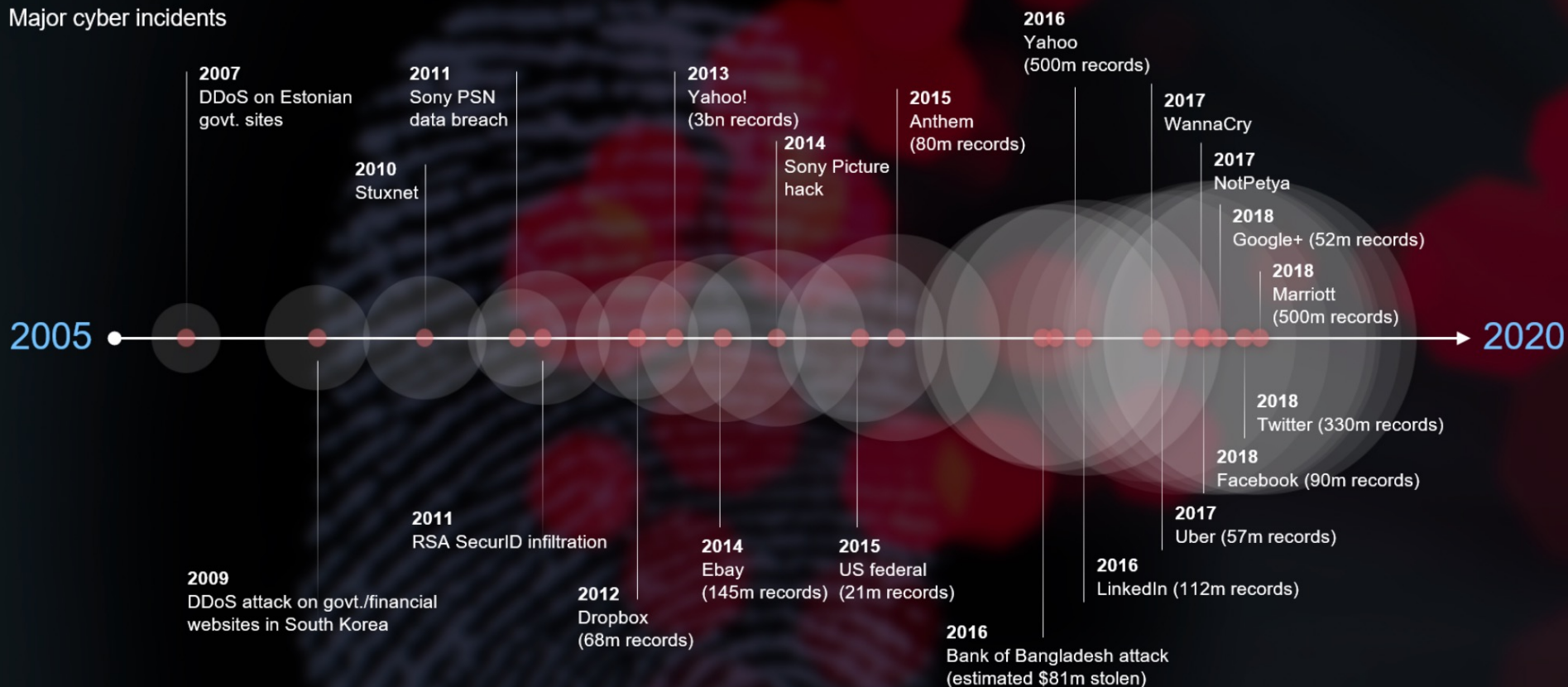


Image: Andrew Brookes / Getty Images

Source: <https://www.munichre.com/en/risks/cyber-risks.html>

20K - 40K

Estimated # of
Paycheck-Collecting
Nation State Offensive Hackers Worldwide



“It takes 20 years to build a reputation
and five minutes to ruin it.”

Warren Buffett

What We'll Talk About

- Big Picture
- Few Startup Axioms
- Privacy
- Security
- Questions



Big Picture

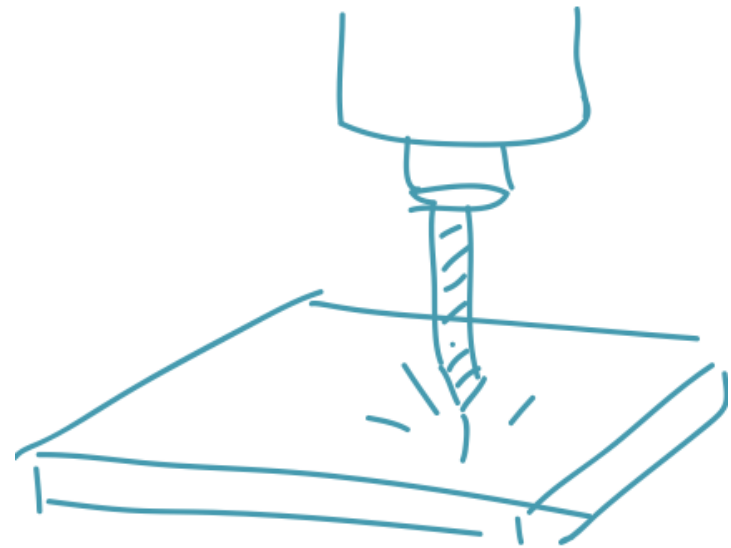




So, how does this apply to startups?



Axiom 1: Focus



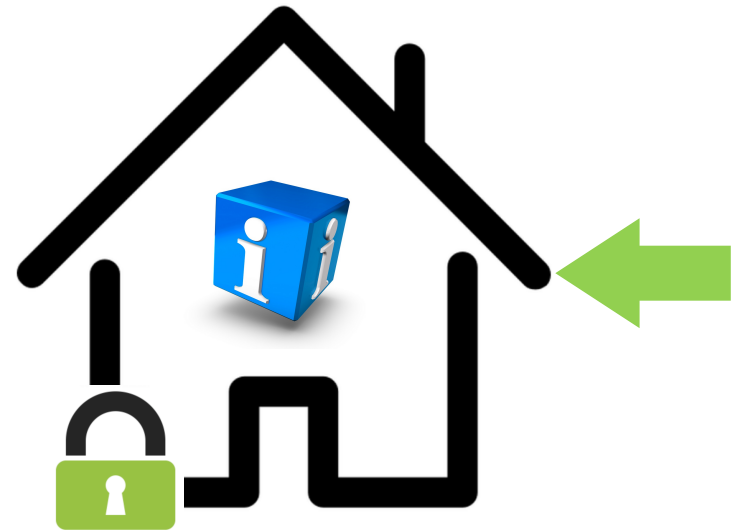
Axiom 2: Stage Appropriateness



Axiom 3: Find trustworthy trail guides early



Privacy



A Sea Change Starting in 2018

For example...

- Privacy Management Platform
- Founded 2016
- Today
 - 2,700 Employees
 - \$4.5B valuation as of July 2023



Context

- Ever Increasing Digitalization of Life
- Cloud Computing → Democratizing Big Data
- GDPR & CCPA ... and numerous others...
- AI
- No System is 100% Secure



Regulations and Trends

- There Are Many, It's Sort of a Mess
- Some Key Regulations To Be Aware Of
 - State-level Data Breach Laws
 - General Data Protection Regulation (GDPR), Digital Services Act (DSA)
 - Fair Credit Reporting Act (FCRA)
 - Gramm-Leach-Bliley
 - Can Spam Act
 - Telephone Consumer Protection Act
 - Children's Online Privacy Protection Act (COPPA)
 - Health Insurance Portability and Accountability Act (HIPPA)
 - Federal Election Commission
- Trends
 - National "GDPR-like" Regulation Coming to U.S.
 - California Consumer Privacy Act (CCPA & CPRA)





Making Sense of It All

- Minimize what you collect
- Handle sensitive data with care
- Carefully evaluate privacy trade-offs
- Diligently protect



Key Concepts In CCPA

- Right to access
- Right to deletion
- Right to knowing if sold, and for what purpose
- Right to opt out



US State Privacy Legislation Tracker 2025



Comprehensive Consumer Privacy Bills

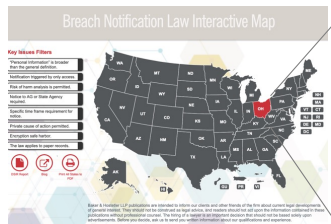
														Consumer rights				Business obligations							
														Right to access	Right to correct	Right to delete	Right to opt out of certain processing	Right to portability	Right to opt out of sales	Right to opt in for sensitive data processing	Right against automated decision-making	Private right of action	Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments
State	Legislative process	Statute/bill	Common name																						
LAWS SIGNED (TO DATE)																									
California							CCPA	California Consumer Privacy Act (2018; effective 1 Jan. 2020)	X	X	X	S	X	X		X	L	16	X	X	X	X			
Colorado							SB 190	Colorado Privacy Act (2021; effective 1 July 2023)	X	X	X	P	X	X	X	X~		S/13	X	X	X	X			
Connecticut							SB 6	Connecticut Data Privacy Act (2022; effective 1 July 2023)	X	X	X	P	X	X	X	X~		S/13	X	X	X	X			
Delaware							HB 154	Delaware Personal Data Privacy Act (2023; effective 1 Jan. 2025)	X	X	X	P	X	X	X	X		17	X	X	X	X			

Source: <https://iapp.org/resources/article/us-state-privacy-legislation-tracker/>



“Toxic Data” & Data Breach Laws

Breach Notification Law Interactive Map



Key States Filter:


- Personal Information (PI) Laws
- PI Laws with Financial Data
- PI Laws with Health Information
- PI Laws with Other Data
- PI Laws with All Data

Map of the United States with states color-coded by their breach notification laws. Ohio is highlighted in red.

BakerHostetler
Ohio

Ohio Rev. Code Ann. §§ 1347.12 (state agencies), 1349.19 (persons and businesses), 1349.191–192 (2007)


Download



Personal Information (i.e., “Personal Identifying Information”)

An individual's first name or first initial with last name with one of the following identifiers:

1. Social Security number.
2. Driver's license or identification card number.
3. Account number, credit or debit card number, in combination with and linked to any required security or access code, or password that would permit access to an individual's financial account.

Persons Covered

Any person, including any business that is conducted in Ohio and that owns, licenses or maintains computerized data that includes personal information.

Any state agency or agency of a political subdivision.

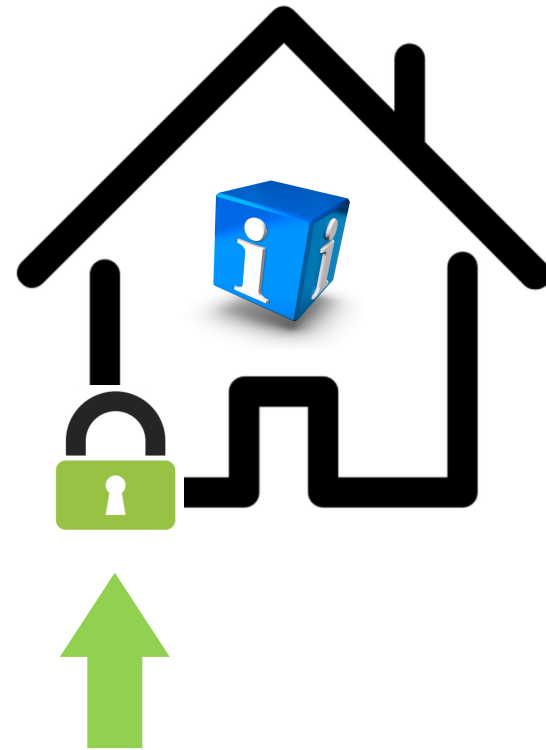
Encryption/Notification Trigger

If the data is encrypted, redacted or altered by any method or technology in such a



<https://www.bakerlaw.com/BreachNotificationLawMap>

Security



v2.5

Network Analysis & Forensics

AWAKE COS cloudthink CORE SECURITY Corvil DARKTRAC Fidelis Lumeta NETSCOUT INQUEST palantir PROTECTWAVE SEC SSR utimaco VECTRA

Endpoint Prevention

AhnLab, avast, Aveo, Avira, Bkaly, Carbon Black, Check Point, Cisco, Cylance, ESET, Fortinet, HIPS, McAfee, Microsoft, Panda, Sophos, Symantec, Trend Micro, VirusBolt, Webroot, Zscaler.

Endpoint Detection & Response

Belcan, Bitdefender, Cynet, Cyren, Cyware, Emsisoft, ESET, Fortinet, HIPS, McAfee, Microsoft, Panda, Sophos, Symantec, Trend Micro, VirusBolt, Webroot, Zscaler.

Cloud Managed Security

Avast, Avira, Bkaly, Carbon Black, Check Point, Cisco, Cylance, ESET, Fortinet, HIPS, McAfee, Microsoft, Panda, Sophos, Symantec, Trend Micro, VirusBolt, Webroot, Zscaler.

[illegible]

The diagram illustrates the relationship between Data Privacy and Data Centric Security. On the left, under the heading "Data Privacy", are logos for COVARTA, D:DAY LABS, OneTrust, and SPION. On the right, under the heading "Data Centric Security", are logos for BlueTalon, CODE42, Dattex, dataphy, NetScout, CitrusCM, egress, global security, IONIC, PRIVYTR, SECLORE, SPIRION, StorageCraft, FRIMARK, VARONIS, and VERA.

IBM
 BLACKSTRATUS CORELOGIX CYBERANT
 DEVO DEVOPS DPIPE EventTracker EXABEAM
 FORINNET HANSIGHT HUNTSMAN KALIDEX IBM JASK
 logtenres logpoint logRhythmic logix.io McAfee
 MICROSOFT Palantir RSA SUNMILL SECURIXONIX
 solarwinds splunk sumologic TIBCO Trustwave

IoT Devices

AGARI Astaro Astaro IDB STREETS

Baracoda Cisco Clearwire Cybex

Canvax Cengage EdgeWave FireEye Forcepoint

Fitbit GreatHorn GWAVE Inky

Homecast PHISHLABS Proofpoint SaaS Software

SonicWall Sophos Spamina Symantec

Trend Micro Trustwave CodeSecure MailMall

Vioto Webroot Wicr

Connected Home

AGARI Astaro Astaro IDB STREETS

Baracoda Cisco Clearwire Cybex

Canvax Cengage EdgeWave FireEye Forcepoint

Fitbit GreatHorn GWAVE Inky

Homecast PHISHLABS Proofpoint SaaS Software

SonicWall Sophos Spamina Symantec

Trend Micro Trustwave CodeSecure MailMall

Vioto Webroot Wicr

Other

AGARI Astaro Astaro IDB STREETS

Baracoda Cisco Clearwire Cybex

Canvax Cengage EdgeWave FireEye Forcepoint

Fitbit GreatHorn GWAVE Inky

Homecast PHISHLABS Proofpoint SaaS Software

SonicWall Sophos Spamina Symantec

Trend Micro Trustwave CodeSecure MailMall

Vioto Webroot Wicr

The collage features logos for the following companies:

- CyberTruq**
- DPLabs**
- Palo Alto**
- Resilient**
- Shiftr Security**
- SYGN/A**
- DarkLight**
- FireEye**
- Microsoft**
- Rapid7**
- Raytheon**
- ServiceNow**
- Splunk**
- Swimlane**
- ThreatOutlook**
- Uplevel**
- Awake**
- Bay Dynamics**
- DarkTrace**
- Dtex**
- ESENTire**
- Exabeam**
- Fortinet**
- Fluency**
- HanSight**
- Hewlett Packard Enterprise**
- Invision**
- Intersect**
- IronNet**
- Jaspers**
- Lacework**
- Observe IT**
- Patternix**
- RSA**
- Reservoir Labs**
- SecOps**
- Teramind**
- TheTarat**
- VMware**
- Securix**
- Vectra**
- Veriato**
- TripleCyber**

OGD brandprotect. crisp digital shadows...
Digital... N.A.M.O.O.O.O.O. GADIUM
Social... source... ZEROFOX
accutrace...
EY... FireEye...
NEC... OPTI...
Fr...
AUTIX BIOCATCH... FRAUD... Brighter...
First Data... FORTER... GROUP...
NCS... Pondera... riskified...
Guardian...
sift science...

Blockchain

Aventus **ETC** **CORVIO** Deloitte **EMER GROUP**
Bitfury **Bitfury** **leidos** **nccgroup**
WTC **STRONG** **PROSECUTOR** **SYGNA** **WPI**

Blockchain

BLACKBERRY ARMOUR **Chain** **CRAXEL** **edge**
guardtime **IDEE** **Manifold** **NuU**
remme **ShoCard** **evchain** **xage**

& Transaction Security

ADVISOR **EMER** **emessage** **ethoca** **FICO** **feedzai**
enTrust **evm** **Kount** **MagicCube** **NetScouts**
SIGNIFYO **simility** **SOCURE** **TokenID** **ThreatMetrix**
RAKIND **UNIKEN** **technology**

Chain CRAXEL edge
Everlance IDEE Manifold NuID
ShoCard vchain xage
EverCompliant FICO feedzai
MagicCube MAXIMIND UNIKEN NetGuarantians
DealMatrix technology

The diagram illustrates the relationship between Container, Infrastructure, and Cloud Service Providers (CSP). The 'Container' box lists logos for anchore, aqua, camptools, and deepblue. The 'Infrastructure' box lists logos for AWS, Oracle, BetterCloud, BYAKNET, cavinin, Check Point, and Splunk. The 'CSP' box lists logos for Arianet, Bitglass, CipherCloud, Cisco, ESOINET, and Managed Networks. Arrows indicate that Containers are built on Infrastructure, and Infrastructure is provided by CSPs.

A Simple Way of Breaking It Down

	Offense	Defense
Nation-State	✓	✓
Companies & Criminals	Criminals	Companies
Kids in the Basement	✓	--



General Guidelines

- Focus on doing the basics well
- Invest where there is risk



Top 5 Checklist

From Harvard Belfer Center Cybersecurity Campaign Playbook

1. Establish a culture of security awareness
2. Use the cloud
3. Use two-factor authentication
4. Encrypted messaging for sensitive comm.
5. Plan and prepare



Source: <https://www.belfercenter.org/cyberplaybook>

Improving your security **is a process.**
You can take control.
Don't just throw your hands up.



Other Things to Keep in Mind



Be Vigilant of Open Source Tools You Use



Top 10

<https://owasp.org/www-project-top-ten>



Third Party Risk

HubSpot

Software | Pricing | Resources | Partners | About

Your Information is Safe and Available

Data Protection meets high-scale systems

Our products and services are transforming the sales and marketing industries with the Inbound revolution, but the backbone of our success is providing a safe and trustworthy place for marketing and sales data. Protecting your data is our obsession.

Dropbox

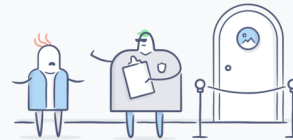
See our plans

At Dropbox, the security of your data is our highest priority

See why millions of people and organizations trust us with their most important work.

Protect your account

Visit the Business Trust Guide



ATLASSIAN

Products | For teams | Support

Try free

Buy now

Join your team

Login

Trust | Security | Reliability | Privacy | Compliance | Platform Roadmap

Security at Atlassian

Security is built into the fabric of our Cloud products, infrastructure, and processes, so you can rest assured that your data is safeguarded.

All security practices



Cloud product security

Security is built into the fabric of our Cloud products. We employ numerous controls to safeguard your data including encryption in transit across our cloud services, external vulnerability research such as our Bug Bounty program, and more.



Security operations and best practices

Our dedicated security team approaches security holistically with a common controls framework. Security threats are prevented using our Atlassian Trust Management System (ATMS), secure



Customers & Partners May Hold You Accountable

- **Limitation of Liability. EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX),** IN NO EVENT SHALL EITHER PARTY BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES, OR DAMAGES FOR LOSS OF PROFITS/REPUTATIONAL HARM, REVENUE, DATA, OR USE, INCURRED BY OTHER PARTY OR ANY THIRD PARTY, WHETHER IN AN ACTION IN CONTRACT OR TORT, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. **EXCEPT WITH RESPECT TO CLAIMS OF INDEMNITY, BREACH OF CONFIDENTIALITY, BREACH OF DATA SECURITY OBLIGATIONS, AND ARISING FROM A DATA INCIDENT (AS SET FORTH IN SECTION XX),** TOTAL LIABILITY FOR A SERVICE IS LIMITED IN ALL CASES AND IN THE AGGREGATE TO THE AMOUNT OF FEES ACTUALLY PAID BY COMPANY FOR THE CORRESPONDING SERVICE DURING THE TWELVE (12) MONTHS PRECEDING THE DATE OF THE EVENT THAT IS THE BASIS FOR THE FIRST CLAIM.



Source: <https://www.winston.com/images/content/1/2/v2/124339/Negotiating-Contractual-Limitations-of-Liability-Provisions-PDF.pdf>

Regulatory Oversight Is On the Horizon

- March 1, 2023 – National Cybersecurity Strategy

**STRATEGIC OBJECTIVE 3.3: SHIFT LIABILITY FOR
INSECURE SOFTWARE PRODUCTS AND SERVICES**

- April 27, 2023 – CISA Attestation Form

Department of Homeland Security

Cybersecurity and Infrastructure Security Agency (CISA)

Secure Software Development Attestation Form Instructions



Frameworks to Know About

- Just to know about...
 - For when your startup scales... not for early-stage
- NIST
 - <https://www.nist.gov/cyberframework>
- System and Organization Controls (SOC)
 - Part of SSAE 16 by American Institute of CPAs
 - <https://www.aicpa.org/soc>



Cyber Risk Insurance



Staying Up to Date

Audio



Email



“Complexity is the worst enemy of security...”

Schneier, Bruce. *Data and Goliath*

Thank You

John Funge

DataTribe

john.funge@datatribe.com

