

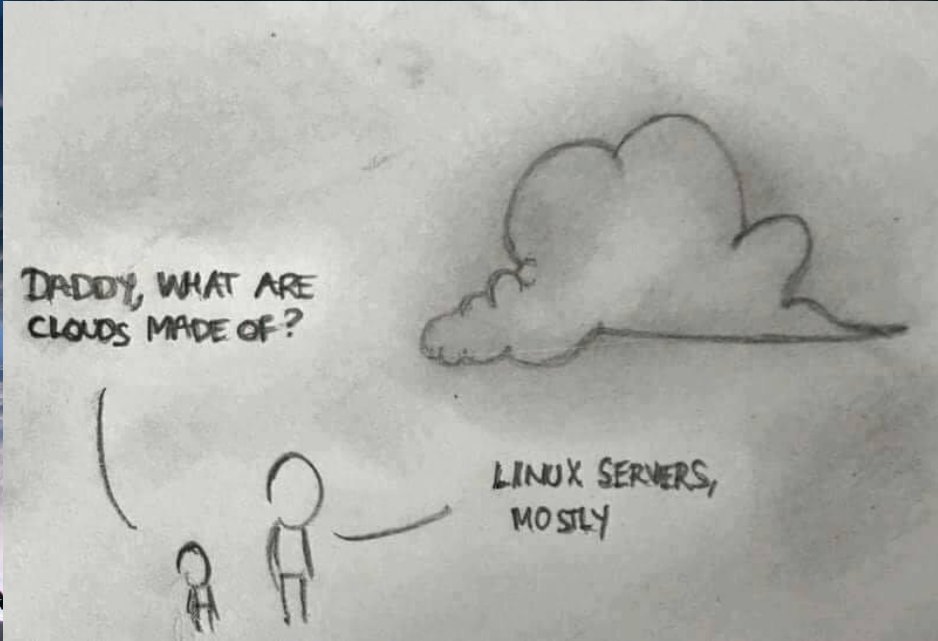


YOUR CLOUD IS

BIGGER THAN YOU THINK



WHAT IS THIS CLOUD?



DADDY, WHAT ARE
CLOUDS MADE OF?

LINUX SERVERS,
MOSTLY

A dramatic photograph of a stormy sky with dark, heavy clouds and bright light breaking through near the horizon. Rain is visible falling in several places. The foreground shows the silhouettes of trees and houses.

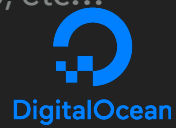
SOMEONE ELSE'S COMPUTER_

A dramatic photograph of a stormy sky with dark, heavy clouds and bright light breaking through near the horizon. Rain is visible falling in several places. The foreground shows the silhouettes of trees and houses.

SOMEONE ELSE....

OBVIOUS CLOUD THINGS

- ▶ File Storage
- ▶ Documents
- ▶ Dropbox, Box, AWS Servers, VPS, etc...



MAYBE NOT AS OBVIOUS

- ▶ Email
- ▶ AD Information
- ▶ DNS

ALSO 'THE CLOUD'

- ▶ Third Parties
 - ▶ Hospitals/Medical
 - ▶ Law
 - ▶ Contractors

EXAMPLE COMPANY: XYZ, INC.

- ▶ Started in 1950
- ▶ Stores everything in the back room
- ▶ 1980: Computers. Transferring things to disk.
- ▶ 1990: Start storing on local file servers
- ▶ 2000: Starts storing on remote file servers.
 - ▶ Outsourcing data storage to other companies
 - ▶ Outsourcing data and information storage to services



EXAMPLE COMPANY: XYZ, INC.

- ▶ Uses a contracting company for services

EXAMPLE COMPANY: XYZ, INC.

- ▶ Uses a contracting company for services

Aug
12
2017

Surgical Dermatology Group notifies patients after TekLinks hacked

“ On June 7, 2017, Surgical Dermatology Group in Birmingham, Alabama (“SDG”) received notice from its cloud hosting and server management provider, TekLinks, Inc., of a security breach at its Birmingham facility that hosts our server. We immediately initiated an investigation and learned that external hackers had gained access to our server possibly as far back as March 23, 2017. TekLinks has assured us that all unauthorized access was terminated on May 1, 2017 and that monitoring by TekLinks from April 22, 2017 through May 1, 2017 showed no further malicious activity during that time period. SDG has worked with the assistance of third-party forensic investigators to determine the full nature and scope of the security incident and to confirm the security of its servers and the integrity of its patient information. We are taking additional steps to ensure the privacy and security of its patients’ information including contacting the Federal Bureau of Investigation.

“ On June 7, 2017, Surgical Dermatology Group in Birmingham, Alabama (“SDG”) received notice from its cloud hosting and server management provider, TekLinks, Inc., of a security breach at its Birmingham facility that hosts our server. We immediately initiated an investigation and learned that external hackers had gained access to our server possibly as far back as March 23, 2017. TekLinks has assured us that all unauthorized access was terminated on May 1, 2017 and that monitoring by TekLinks from April 22, 2017 through May 1, 2017 showed no further malicious activity during that time period. SDG has worked with the assistance of third-party forensic investigators to determine the full nature and scope of the security incident and to confirm the security of its servers and the integrity of its patient information. We are taking additional steps to ensure the privacy and security of its patients’ information including contacting the Federal Bureau of Investigation.

“ On June 7, 2017, Surgical Dermatology Group in Birmingham, Alabama (“SDG”) received notice from its cloud hosting and server management provider, TekLinks, Inc., of a security breach at its Birmingham facility that hosts our server. We immediately initiated an investigation and learned that external hackers had gained access to our server possibly as far back as March 23, 2017. TekLinks has assured us that all unauthorized access was terminated on May 1, 2017 and that monitoring by TekLinks from April 22, 2017 through May 1, 2017 showed no further malicious activity during that time period. SDG has worked with the assistance of third-party forensic investigators to determine the full nature and scope of the security incident and to confirm the security of its servers and the integrity of its patient information. We are taking additional steps to ensure the privacy and security of its patients’ information including contacting the Federal Bureau of Investigation.

EXAMPLE COMPANY: XYZ, INC.

- ▶ Uses a contracting company for services
- ▶ Uses a law firm

EXAMPLE COMPANY: XYZ, INC.

- ▶ Uses a contracting company for services
- ▶ Uses a law firm

May
11
2017

Chinese Hackers Must Pay \$8.9 Million for Law Firm Data Theft

“

Three Chinese hackers who traded on data they stole from two top New York law firms were ordered by a judge to pay \$8.9 million.

U.S. District Judge Valerie Caproni in Manhattan on May 5 fined the men and ordered them to forfeit their profits, plus interest. The hackers, lat Hong, Bo Zheng and Hung Chin, broke into the email accounts of senior lawyers whose firms were hired to advise on corporate mergers and acquisitions, according to the government.

Caproni ordered a default judgement in favor of the Securities and Exchange Commission because the three men didn't appear in court to contest the claims.

“

Three Chinese hackers who traded on data they stole from two top New York law firms were ordered by a judge to pay \$8.9 million.

U.S. District Judge Valerie Caproni in Manhattan on May 5 fined the men and ordered them to forfeit their profits, plus interest. The hackers, Iat Hong, Bo Zheng and Hung Chin, broke into the email accounts of senior lawyers whose firms were hired to advise on corporate mergers and acquisitions, according to the government.

Caproni ordered a default judgement in favor of the Securities and Exchange Commission because the three men didn't appear in court to contest the claims.

“

Three Chinese hackers who traded on data they stole from two top New York law firms were ordered by a judge to pay \$8.9 million.

U.S. District Judge Valerie Caproni in Manhattan on May 5 fined the men and ordered them to forfeit their profits, plus interest. The hackers, Iat Hong, Bo Zheng and Hung Chin, broke into the email accounts of senior lawyers whose firms were hired to advise on corporate mergers and acquisitions, according to the government.

Caproni ordered a default judgement in favor of the Securities and Exchange Commission because the three men didn't appear in court to contest the claims.

THIRD-PARTY BREACHES



MAY, 2017

BRONX LEBANON HOSPITAL
VIA IHEALTH

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

HOW IT HAPPENED

- ▶ Misconfigured Rsync backup server hosted by iHealth
- ▶ Discovered using Shodan

The search engine for

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account

Getting Started



MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

WHAT WAS TAKEN

- ▶ 7,000 people between 2014-2017
- ▶ Names & home addresses
- ▶ Addiction Histories
- ▶ Religious Affiliations
- ▶ Mental Health & Diagnoses
- ▶ HIV Status
- ▶ Sexual Assault Reports
- ▶ Domestic violence Reports



Abuse:
[REDACTED]
Has patient been hit/kicked/slapped or forced to have sex , or is a victim of neglect : yes
Suspected Physical Abuse : no
Suspected Sexual Abuse : no
Suspected Neglect : no
Abuse Reported : no
Case Accepted by ACS/APS : no
Comments: patient was physically abused by [REDACTED] She was raped by her [REDACTED]
SUBSTANCE ABUSE HISTORY:
Substance Abuse Hx:
[REDACTED]
Alcohol/Beer: 2x40oz/ [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Orally.
Cannabis: 1 Joint / [REDACTED] - weekly , Last Used - 4 hour(s) ago , Age of First Use - 14 Years Old , Route of Administration - Smoking.
Cocaine: \$50-100 - weekly , Last Used - 4 hour(s) ago , Age of First Use - [REDACTED] years Old , Route of Administration - Smoking and Nasal (sniffing).
Within the last (6) months, describe triggers/precipitants to use: [REDACTED]
[REDACTED]
Loneliness.
Within the last (6) months, describe pattern of substance use, during a typical week: drinks alcohol, use cocaine, cannabis dependence.
Longest Period of Abstinence: [REDACTED] years.
Conditions Contributing to Abstinence: strong motivation to be clean employed
good family support.
Is Patient currently on Methadone Maintenance: no.
Describe Perceived Negative Consequences of Substance Use: stop medications legal problems.
Describe Perceived Positive Consequences of Substance Use: Patient reports " i enjoy it".

WHAT THEY DID WRONG

- ▶ Bronx Lebanon Outsourced Backups without Audit
- ▶ IHealth Collected Backup Data in an Insecure Manner

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

"AT THIS TIME, IHEALTH BELIEVES THAT THE ISSUE HAS BEEN CONTAINED,"

"IHEALTH HAS NO INDICATION THAT ANY DATA HAS BEEN USED INAPPROPRIATELY."

iHealth

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

HOSPITAL MITIGATIONS

- ▶ Audit their Cloud Providers
- ▶ Perform regular searches for their data using tools like Shodan
- ▶ Perform Vulnerability Analysis
- ▶ Encrypt their data

MAY, 2017: BRONX LEBANON HOSPITAL CENTER (NY)

IHEALTH MITIGATIONS

- ▶ Secure Connections
- ▶ Perform Regular Searches Using Tools Like Shodan
- ▶ Conduct Vulnerability Analysis
- ▶ Require Data Encryption

AUGUST, 2017

NHS PATIENT DATA VIA SWIFTQUEUE

<https://www.thesun.co.uk/tech/4274225/anonymous-hacker-claims-to-have-stolen-the-nhs-medical-records-of-1-2million-brits/>

HOW IT HAPPENED

- ▶ Exploited Vulnerabilities in SwiftQueue's Software

NHS HACK ATTACK Anonymous hacker claims to have stolen private data on up to 1.2million NHS patients

NHS/SWIFTQUEUE

- ▶ Hacker: 1.2 Million NHS Patient Records
- ▶ Company: 32,501 Patient Records

WHAT WAS TAKEN

- ▶ Names
- ▶ DOB
- ▶ Phone Numbers
- ▶ Email Addresses

NHS MITIGATIONS

- ▶ Require Certain Levels of Security from Vendors
- ▶ Encrypt Data

SWIFTQUEUE MITIGATIONS

- ▶ Follow General Security Best Practices
- ▶ Encrypt Data
- ▶ Perform Vulnerability Analysis
- ▶ Keep Systems up to date

A COUPLE OTHER DATA BREACHES



2016/2012

DROPBOX

<https://www.hackread.com/hackers-stole-dropbox-passwords/>

HOW IT HAPPENED

- ▶ 2012 Breach
 - ▶ Old Credentials (emails and hashed passwords)
 - ▶ Users noticed spam emails from email accounts used only for DropBox access
 - ▶ Stolen Password Used to Access Employee Account

WHAT WAS TAKEN

- ▶ 2016
 - ▶ 68,680,741 Account Emails and Hashed Passwords
 - ▶ 32 Million Passwords used bcrypt
 - ▶ The Rest Used SHA1, but with a salt

DROPBOX RESPONSE

- ▶ Suggested Two-Factor
- ▶ Added New Automated Mechanisms to Detect Suspicious Behavior
- ▶ Created a Page to Check Active Logins
- ▶ Required Password Resets

TAKE-AWAYS

- ▶ Enable Two-Factor or more
- ▶ Check Active Logins
- ▶ Change Password Often



JULY, 2015

ASHLEY MADISON

<https://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/>

JULY, 2015, ASHLEY MADISON DATA BREACH

HOW IT HAPPENED

- ▶ Impact Team
- ▶ Databases were accessed
- ▶ Website may have been vulnerable
- ▶ Could have been malware

WHAT WAS TAKEN

- ▶ 27.5 Million Users Affected
 - ▶ Real Names
 - ▶ Addresses
 - ▶ Credit Card Numbers
 - ▶ Sexual Fantasies

WHAT WAS TAKEN

- ▶ Internal Company Servers
- ▶ Employee Account Information
- ▶ Company Bank Account Data
- ▶ Salary Information
- ▶ Employee Emails

TERRIBLE RESPONSE

- ▶ Lots of Denial
- ▶ 60 GB of data confirmed on Aug 18
 - ▶ Released on bittorrent, shared in the Dark Web

TIME'S UP!

Avid Life Media has failed to take down Ashley Madison and Established Men. We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data.

Find someone you know in here? Keep in mind the site is a scam with thousands of fake female profiles. See ashley madison fake profile lawsuit; 90-95% of actual users are male. Chances are your man signed up on the world's biggest affair site, but never had one. He just tried to. If that distinction matters.

Find yourself in here? It was ALM that failed you and lied to you. Prosecute them and claim damages. Then move on with your life. Learn your lesson and make amends. Embarrassing now, but you'll get over it.

Any data not signed with key 6E50 3F39 BA6A EAAD D81D ECFF 2437 3CD5 74AB AA38 is fake.

[Impact Team's statement on the release](#)

[Impact Team's PGP signature for the released statement](#)

[Impact Team's PGP Key](#)

[Torrent for the released data](#)

[Back to Quantum Magazine](#)

JULY, 2015, ASHLEY MADISON DATA BREACH

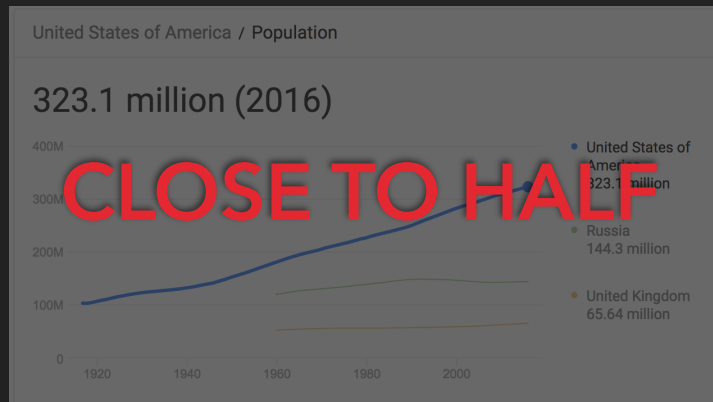
Name	Size	Have	Download	Priorit
▼ srcdmp	19.92 GB	0 %	✓	Norma
ashleymadison.tgz	3.43 GB	0 %	✓	Norma
avid.tgz	57.78 MB	0 %	✓	Norma
dba.tgz	210.0 MB	0 %	✓	Norma
design.tgz	337.1 MB	0 %	✓	Norma
dev.tgz	534.0 MB	0 %	✓	Norma
misc.tgz	344.3 MB	0 %	✓	Norma
mobile.tgz	863.6 MB	0 %	✓	Norma
noel.biderman.mail.7z	13.74 GB	0 %	✓	Norma
noel.biderman.mail.7z.asc	0.84 kB	0 %	✓	Norma
product.tgz	203.3 MB	0 %	✓	Norma
qa.tgz	32.69 MB	0 %	✓	Norma

SEPT, 2017

EQUIFAX

WHO IS AFFECTED

- ▶ 143 Million Customers



HOW IT HAPPENED

- ▶ Vulnerable Web App on a US Website
 - ▶ Old Apache Struts Vulnerability

WHAT WAS TAKEN

- ▶ Names
- ▶ Birth Dates
- ▶ Phone Numbers
- ▶ Email Addresses
- ▶ Credit Card Info from 209,000 Customers
- ▶ Dispute Docs with PII for 182,000 Customers
- ▶ SSN's



WHAT WAS TAKEN

- ▶ Names
- ▶ Birth Dates
- ▶ Phone Numbers
- ▶ Email Addresses
- ▶ Credit Card Info from 209,000 Customers
- ▶ Dispute Docs with PII for 182,000 Customers
- ▶ SSN's

Everything you need
for Identity Theft!

POOR RESPONSE

- ▶ Attackers had access mid-May to July 2017
- ▶ Breach discovered July 29
- ▶ *Three executives (including CFO) sell a bunch of stock after discovery*
- ▶ We find out about it Sept 7!



WHAT ARE YOUR OPTIONS?

- ▶ Free Credit Monitoring
- ▶ ...from Equifax



POOR RESPONSE

Details for www.equifaxsecurity2017.com

Classifier prediction: suspicious Umbrella risk score: **67**

DNS queries

The graph displays DNS query volume over time. The x-axis represents dates from August 12 to September 7. The y-axis represents the number of DNS queries per hour, ranging from 0 to 150,000. The data shows a significant increase in queries starting around September 6, peaking at approximately 120,000 queries per hour on September 7.

Date	DNS queries / hour (approx.)
12. Aug	0
14. Aug	0
16. Aug	0
18. Aug	0
20. Aug	0
22. Aug	0
24. Aug	0
26. Aug	0
28. Aug	0
30. Aug	0
1. Sep	0
3. Sep	0
5. Sep	0
7. Sep	120,000

POOR RESPONSE

[illegible]



Data Breach Services

Member Center Login

[About Equifax](#) \ [Investors](#) \ [Online Dispute](#) \ [Contact Us](#)

Search

Have a Promo Code? [Click Here](#)



Think your business is safe from a data breach? Think again.

"More than ever before, your employees and customers are at great risk for identity theft and fraud. Over 165 million data records of U.S. residents have been exposed due to data breaches since January 2005 - Privacy Rights Clearinghouse"

Take Action Today: E-mail us at: psol@equifax.com Or call us at: 1-866-510-4211

Data Breaches are on the rise. Be prepared.

You'll feel safer with Equifax. We're the leading provider of data breach services, serving more than 500 organizations with security breach events everyday. In addition to extensive experience, Equifax has the most comprehensive set of identity theft products and customer service coverage in the market.

Hear what our valued customers are saying about our services.

Thank you both very much for the time and effort you provided to assist us in managing our incident. I was very

';--have i been pwned?

Check if you have an account that has been compromised in a data breach


pwned?

233
pwned websites

4,729,225,727
pwned accounts

54,521
pastes

51,631,016
paste accounts

























HomeNotify meDomain searchWho's been pwnedPasswordsAPIAboutDonate

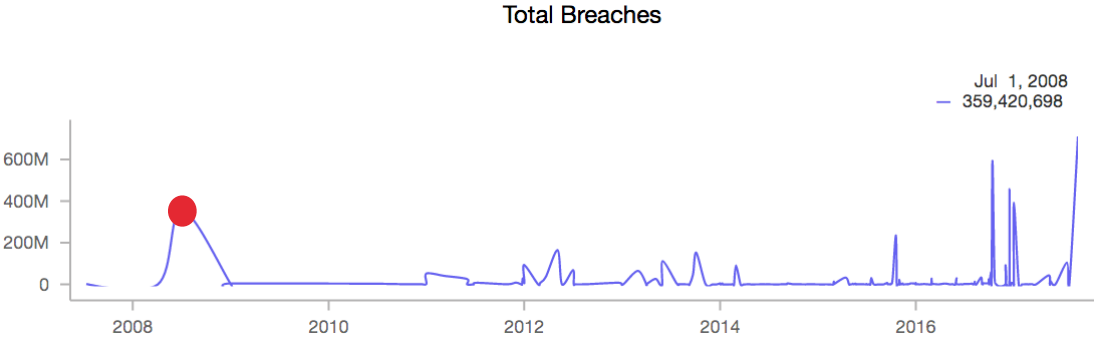
Pwned websites

Breached websites that have been loaded into this service

Here's an overview of the various breaches that have been consolidated into this site. Each of these has been dumped publicly and is readily available via various sites on the web. This information is also available via an [RSS feed](#).

	711,477,622	Onliner Spambot accounts		819,478	Warframe accounts
				800,157	Onverse accounts
	593,427,119	Exploit.In accounts ?		790,724	Brazzers accounts ?
	457,962,538	Anti Public Combo List accounts ?		777,387	Black Hat World accounts
	393,430,309	River City Media Spam List accounts		776,125	Abandonia accounts
				745,355	Android Forums accounts
	359,420,698	MySpace accounts		738,556	WildStar accounts
	234,842,089	NetEase accounts ?		735,405	MALL.cz accounts
	164,611,595	LinkedIn accounts		707,432	Programming Forums accounts
	152,445,165	Adobe accounts		699,793	mSpy accounts
	112,005,531	Badoo accounts ?		657,001	Delicious accounts

myspace.com:
Email Addresses, Usernames, Passwords



LinkedIn:

Email Addresses, Passwords

Total Breaches



Using data from <https://haveibeenpwned.com/>

Dropbox:

Email Addresses, Passwords

Total Breaches



Using data from <https://haveibeenpwned.com/>

tumblr:

Email Addresses, Passwords

Total Breaches



Using data from <https://haveibeenpwned.com/>

adobe:

Email addresses, Password hints, Passwords, Usernames

Total Breaches



Using data from <https://haveibeenpwned.com/>

rivercitymediaonline.com:

Email addresses, IP addresses, Names, Physical addresses

Total Breaches



Using data from <https://haveibeenpwned.com/>

Onliner Spambot :

Email Addresses, Passwords

Total Breaches



Using data from <https://haveibeenpwned.com/>



**HOW DO YOU PROTECT YOUR DATA AGAINST
THIRD PARTY COMPROMISE?**



GENERAL SECURITY STUFF

TRADITIONAL MODELS

- ▶ Firewall
- ▶ IDS
- ▶ Server Configuration
- ▶ AntiVirus
- ▶ Cloud Security
- ▶ Vulnerability Analysis

TRADITIONAL MODELS

- ▶ Firewall
 - ▶ Block External Access on Ports
 - ▶ Secure Connections between Locations

TRADITIONAL MODELS

- ▶ IDS
 - ▶ Searching for known threats on the network
 - ▶ Reporting what you are at risk for

TRADITIONAL MODELS

- ▶ Server Configuration
 - ▶ Separating databases from web front-ends
 - ▶ Securing the connections between servers
 - ▶ Keeping software updated
 - ▶ Limiting Access
 - ▶ Penetration Testing

TRADITIONAL MODELS

- ▶ AntiVirus
 - ▶ Keeping it updated

TRADITIONAL MODELS

- ▶ Cloud Security
 - ▶ Using Services/Companies
 - ▶ Auditing

TRADITIONAL MODELS

- ▶ Vulnerability Analysis
 - ▶ Scanning your environment
 - ▶ Looking for Vulnerabilities



SECURING 'YOU'

MAPPING TO TRADITIONAL MODELS

- ▶ Firewall
- ▶ IDS
- ▶ Server Configuration
- ▶ AntiVirus
- ▶ Cloud Security
- ▶ Vulnerability Analysis

MAPPING TO TRADITIONAL MODELS

- ▶ Firewall
 - ▶ Freeze Your Credit
 - ▶ Keep your computer patched

MAPPING TO TRADITIONAL MODELS

- ▶ IDS
 - ▶ Sign up for services like haveibeenpwnd.com
 - ▶ Set up Google Alerts
 - ▶ Automatic Shodan Searches (Using API)

MAPPING TO TRADITIONAL MODELS

- ▶ ~~Server~~ System Configuration
 - ▶ Use disk encryption & Strong password
 - ▶ Frequent offline backups (on an encrypted drive)
 - ▶ Disable unneeded services
 - ▶ Lock System
 - ▶ Keep it up to date

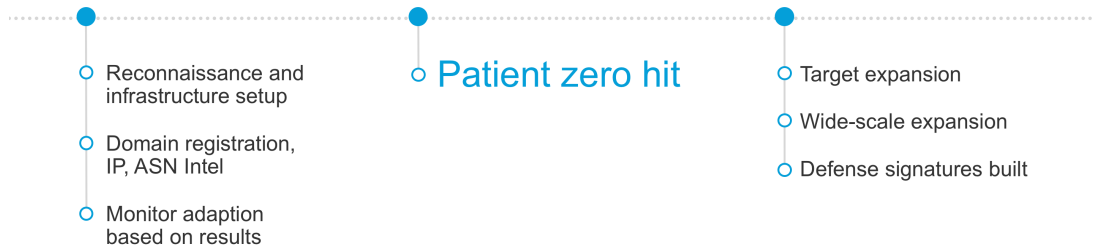
MAPPING TO TRADITIONAL MODELS

- ▶ AntiVirus
 - ▶ Be wary of clicking on links in suspicious emails
 - ▶ Don't install without thinking first
 - ▶ Send that attachment to VirusTotal if unsure

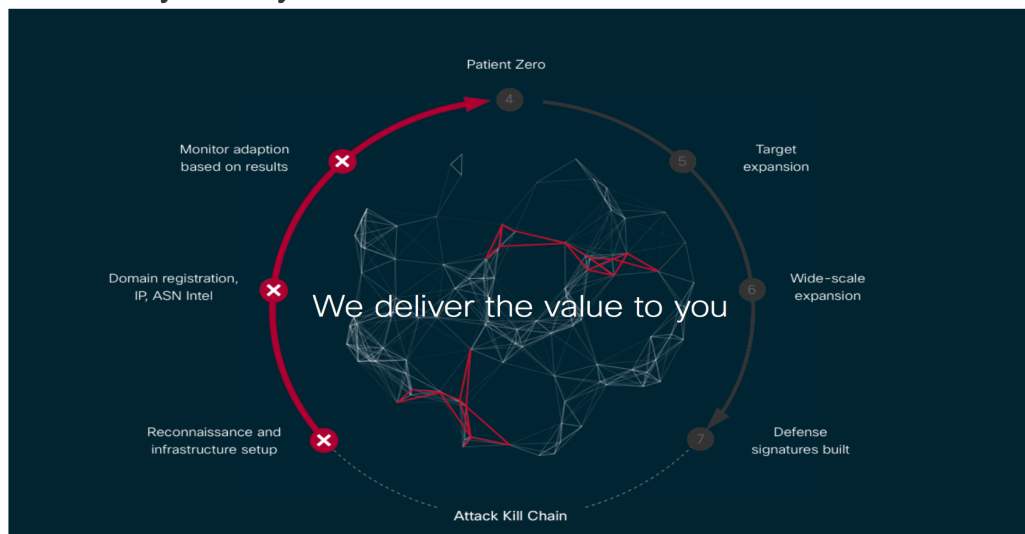
MAPPING TO TRADITIONAL MODELS

- ▶ Cloud Security
 - ▶ Enable two-factor authentication for all Cloud Services
 - ▶ Use additional encryption
 - ▶ Utilize Cool Products

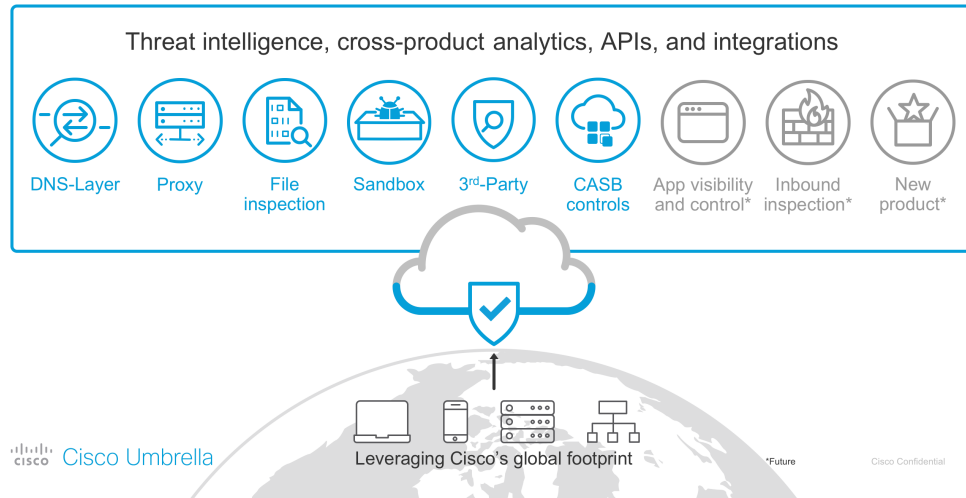
Anatomy of a cyber attack



Anatomy of a cyber attack

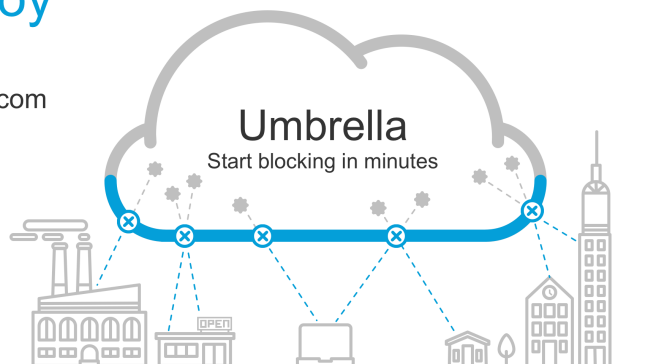


Cisco's Secure Internet Gateway Vision



Easiest security product you'll ever deploy

- 1 <http://signup.umbrella.com>
- 2 Point your DNS: 208.67.222.222
- 3 Done





SECURING YOUR VENDORS

SECURING YOUR VENDORS

- ▶ Research the Company
- ▶ Talk to them about security
 - ▶ How do they store your data?
 - ▶ When must they report a breach?
- ▶ Give them only what you have to
- ▶ Look into Cyber Insurance

Vendor Management



Topics for Discussion

Vendor management best practices

Assess the cybersecurity of vendors

Ongoing monitoring

Recent regulatory developments

Why have a Vendor Management Program?

Legal Obligations

Vendor oversight may be legally required (more on this later). Companies interested in cross-border transfer must pay attention to acceptable mechanisms under international regimes. Finally, contracts may require oversight of subcontractors.



Corporate Success

While you can delegate authority, you cannot delegate accountability. Vendors help provide efficiencies that your organization might not be able to execute, but vendors must achieve expected performance.

Fiscal Oversight

Assessing vendors initially and throughout relationship helps establish expectations and identify problems quickly, which will help cut costs of reacting to any issues.

Best Practices

1

Comprehensive inventory

Catalog all third parties with whom the company has a relationship

2

Risk-based segmentation

Triage vendors to make sure the most effort is devoted to the highest risks

3

Governance framework

Establish owners and give the group the decision-making authority to escalate as problems arise

4

Due Diligence

Questionnaire should be tailored to activity and type of data collected

Assessing the Cybersecurity of Vendors

- Accept the risk or require remediation
- Identify and assess critical, downstream vendors or subcontractors
- Retain all assessment data, decisions, and records
- Ongoing monitoring:

Performance measurements	Audits	Independent verification
<ul style="list-style-type: none">• ROI• New technology assessment• Status assessment	<ul style="list-style-type: none">• Desk audits• In person	<ul style="list-style-type: none">• Third party reports• Certifications• Standards• SOC2

Managing Vendor Contracts

Ideally, management of contracts involving or affecting sensitive or regulated data should be:

- Centralized
 - Avoid bifurcated process for reviewing data security agreement and the underlying service agreement
 - Repetition helps refine approach and improve skill
- Risk-based
 - Tiered approach to allocation of review resources may save expenditure of resources, however, cannot be based on "dollar value of the contract"
- Involve a multi-disciplinary review process
 - Security team review important step – not only expertise, but also ability to spot interplay with other arrangements, products, etc.
 - Need review by attorney(s) with expertise in security

Managing Vendor Contracts: Eating the Elephant

- Identify your organization's full scope of dependencies on third-party service providers or vendors that collect, access, process, disclose, transmit, or host sensitive or confidential data
- Develop formal privacy and data security vendor management processes, such as:
 - Vendor due diligence process (consider a "disclosure" form for vendors to complete prior to review of service agreement)
 - Standard contract terms that complement the organization's privacy and information security programs
 - Review process with multi-disciplinary team with adequate training regarding standards and risk areas
 - Vendor oversight and contract enforcement (consider contract termination procedures to ensure data returned or destroyed; annual review process to validate security warranties; review of arrangements after security incident, etc.)
 - Maintain vendor contact information and ensure key vendors are represented and included as part of incident response team

Most Recent Regulatory Developments

**23 NYCRR
500**
(March 1,
2017)

Implement written policies / procedures designed to ensure the security of information systems and non-public information that are accessible to, or held by Third-Party Service Providers.

**OCC
Bulletin
2017-21**
(June 7,
2017)

OCC issued Bulletin 2017-21 as a supplement to the OCC's 2013 risk management guidance related to third party relationships. Bulletin addresses 14 FAQs related to (i) interpretations of Bulletin 2013-29's scope and content, including applicability to bank relationships with fintech companies; (ii) opportunities for banks to collaborate with each other to manage third party relationships; and (iii) outside resources that banks may use to augment third party risk management capabilities.

GDPR
(May 25,
2018)

Controllers liable for the actions of the processors they select. Can only use processors that provide sufficient guarantees of their abilities to meet GDPR requirements. Controllers should consider data protection impact assessment on processors.

Thank You

CONTACT US:

Jennifer Rathburn
jrathburn@foley.com

Joshua Pyorre
jpyorre@cisco.com

ATTORNEY ADVERTISEMENT. The contents of this document, current at the date of publication, are for reference purposes only and do not constitute legal advice. Where previous cases are included, prior results do not guarantee a similar outcome. Images of people may not be Foley personnel.
© 2017 Foley & Lardner LLP

 **FOLEY**
FOLEY & LARDNER LLP