

Manufacturing Security: Cost Effective Cybersecurity for the Steel Industry




 View Report  View on Map

New Service: Keep track of what you have connected to the Internet. Check out [Shodan Monitor](#)

80.88.90.225

host225-90-88-80.serverdedicati.aruba.it

Aruba S.p.A. - Cloud Services Farm2

 Italy, Arezzo

```
HTTP/1.1 200 OK
Date: Mon, 11 Apr 2022 19:00:24 GMT
Server: Apache/2.4.41 (Ubuntu)
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
Vary: Accept-Encoding
Content-Length: 3280
Content-Type: text/html; charset=UTF-8
```

```
<!DOCTYPE html>
<html lang="it..."
```

192.203.155.39

performanceaero.com

cookware

 United States, Cincinnati

```
HTTP/1.1 200 OK
Date: Mon, 11 Apr 2022 18:12:43 GMT
Server: Apache/2.4.25 (Debian)
Vary: Accept-Encoding
Connection: close
Transfer-Encoding: chunked
Content-Type: text/html; charset=UTF-8
```

```
74f
```

```
<html><head><title>Performance Aero, Inc.</title><SGMETASIG><META NAME="description" CONTENT="..."
```

What we'll cover

- **Why manufacturing is a major target**
- **The threat landscape**
- **The law: Compliance vs Protection**
- **Perato Principle for cyber security**

Why the sector is a major target

April 2019



CISA
CYBER + INFRASTRUCTURE

National Critical Functions Set

National Critical Functions: The functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

SUPPLY

- Exploration and Extraction Of Fuels
- Fuel Refining and Processing Fuels
- Generate Electricity
- Manufacture Equipment
- Produce and Provide Agricultural Products and Services
- Produce and Provide Human and Animal Food Products and Services
- Produce Chemicals
- Provide Metals and Materials
- Provide Housing
- Provide Information Technology Products and Services

Why the sector is a major target

#1

Manufacturing industry rank for attacks

Manufacturing replaced financial services as the top attacked industry in 2021, representing 23.2% of the attacks X-Force remediated last year. Ransomware was the top attack type, accounting for 23% of attacks on manufacturing companies.

Cyber attacks on manufacturing up 300% in a year

NTT also found that application-specific and web-application attacks accounted for two-thirds of all cyber crime

CYBER THREATS TO CRITICAL MANUFACTURING SECTOR INDUSTRIAL CONTROL SYSTEMS (ICS)

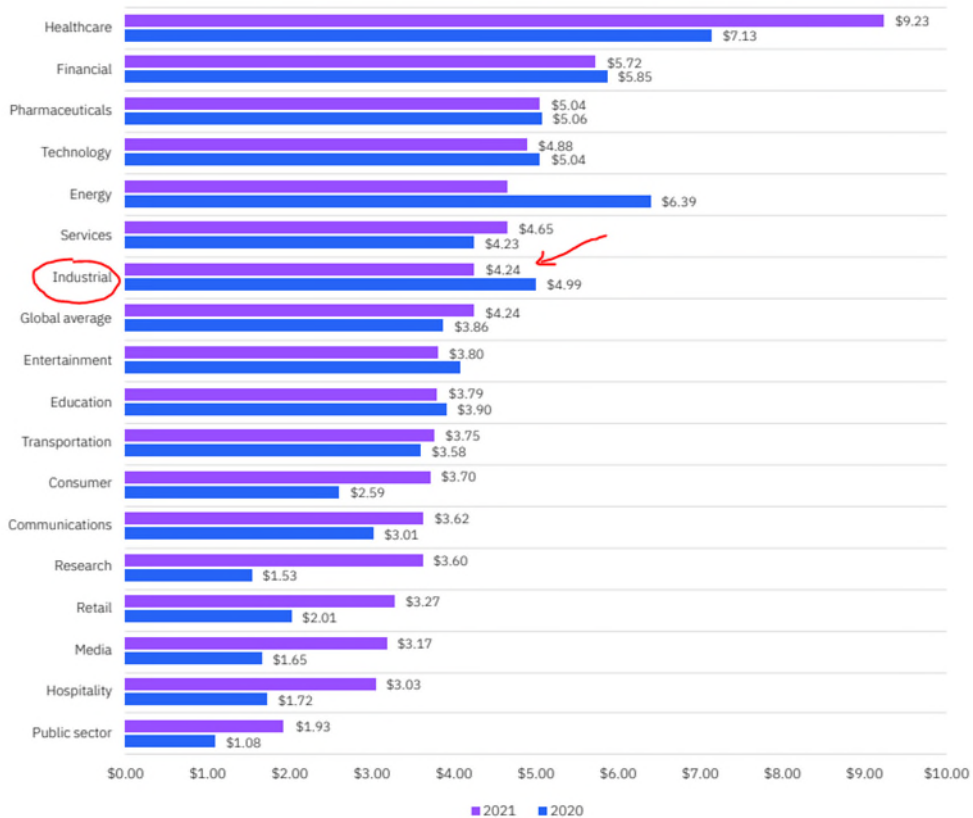
The Critical Manufacturing Sector is at risk from increased cyber-attack surface areas and limited cybersecurity workforces related to the COVID-19 pandemic. These trends increase the vulnerability¹ of the Critical Manufacturing Sector to the growing number of ransomware attacks aimed at private businesses by increasing attack surfaces and reducing protective abilities. To mitigate future threats, the Critical Manufacturing Sector should prioritize the management of risks.

Why the sector is a major target

Figure 4

Average total cost of a data breach by industry

Measured in US\$ millions



Why the sector is a major target

Manufacturing presents a (relatively) low risk / high reward environment for cybercrime:

- more “attack surfaces” (IT/OT)
- budget priorities
- business priorities (safety / QA)
- workforce busy with “real work”



"I'm sure there are better ways to disguise sensitive information, but we don't have a big budget."

The threat landscape

Vector vs Goal

Vectors

- disgruntled workforce
- RAT
- social engineering
- BEC
- stolen credentials
- purchased credentials
- ransomware

Goals

- system damage
- reputational damage
- data theft
- credential harvesting
- money

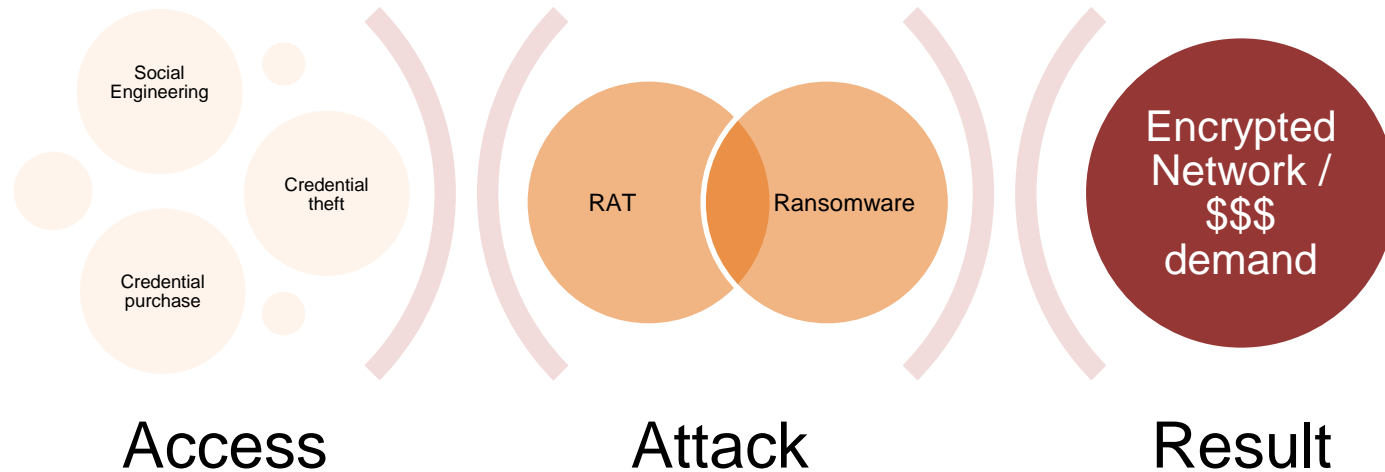
© Randy Glasbergen
www.glasbergen.com



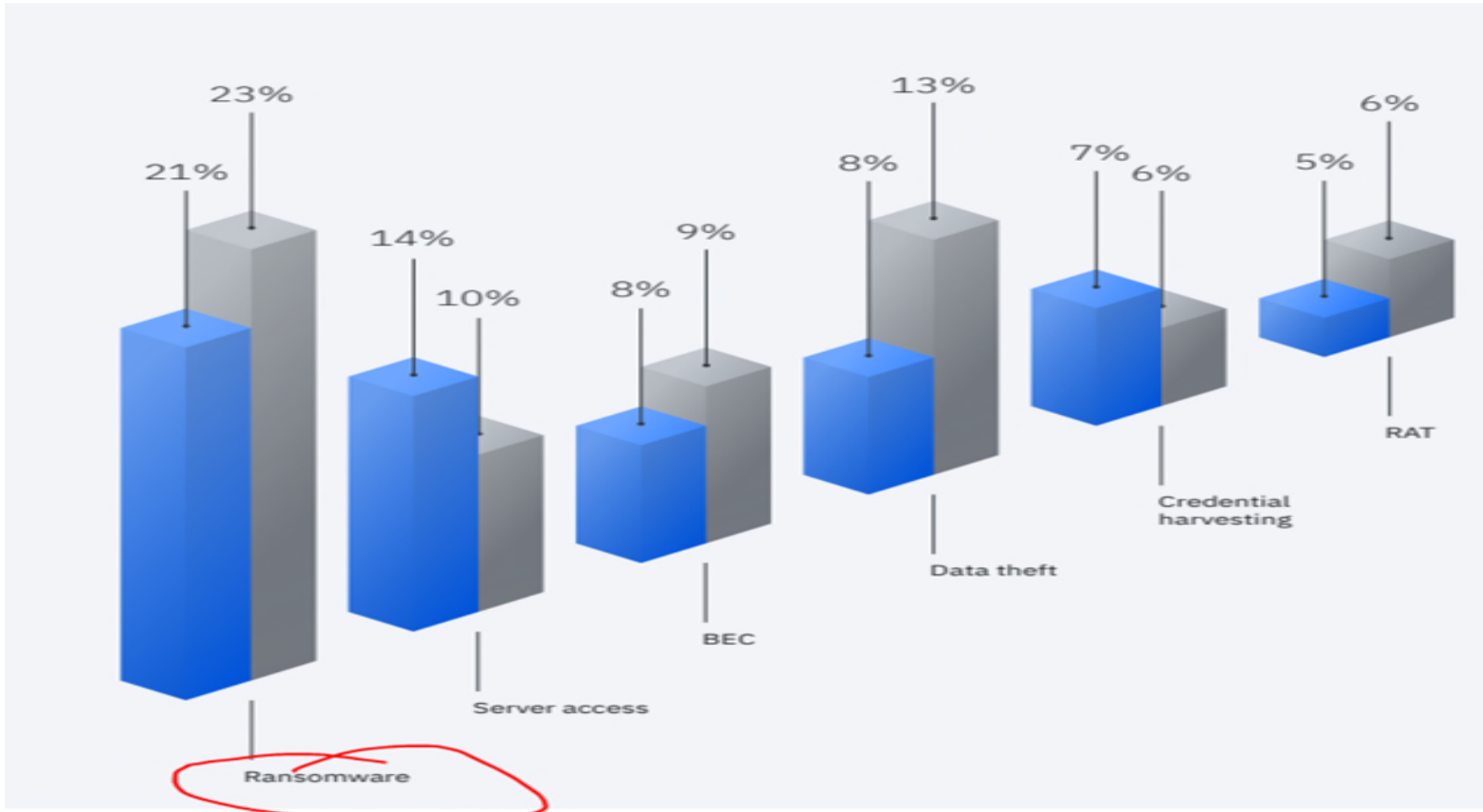
"I keep our secure files in a coffee can buried behind the office. You can't hack into that with a computer!"

The threat landscape

Most attacks are multi-vector



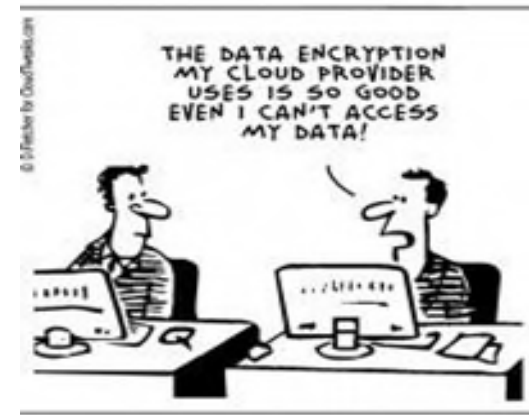
The threat landscape (all industries)



The threat landscape

Leading vectors for manufacturing:

- **ransomware**
- **business email compromise**



The threat landscape – BEC Attack

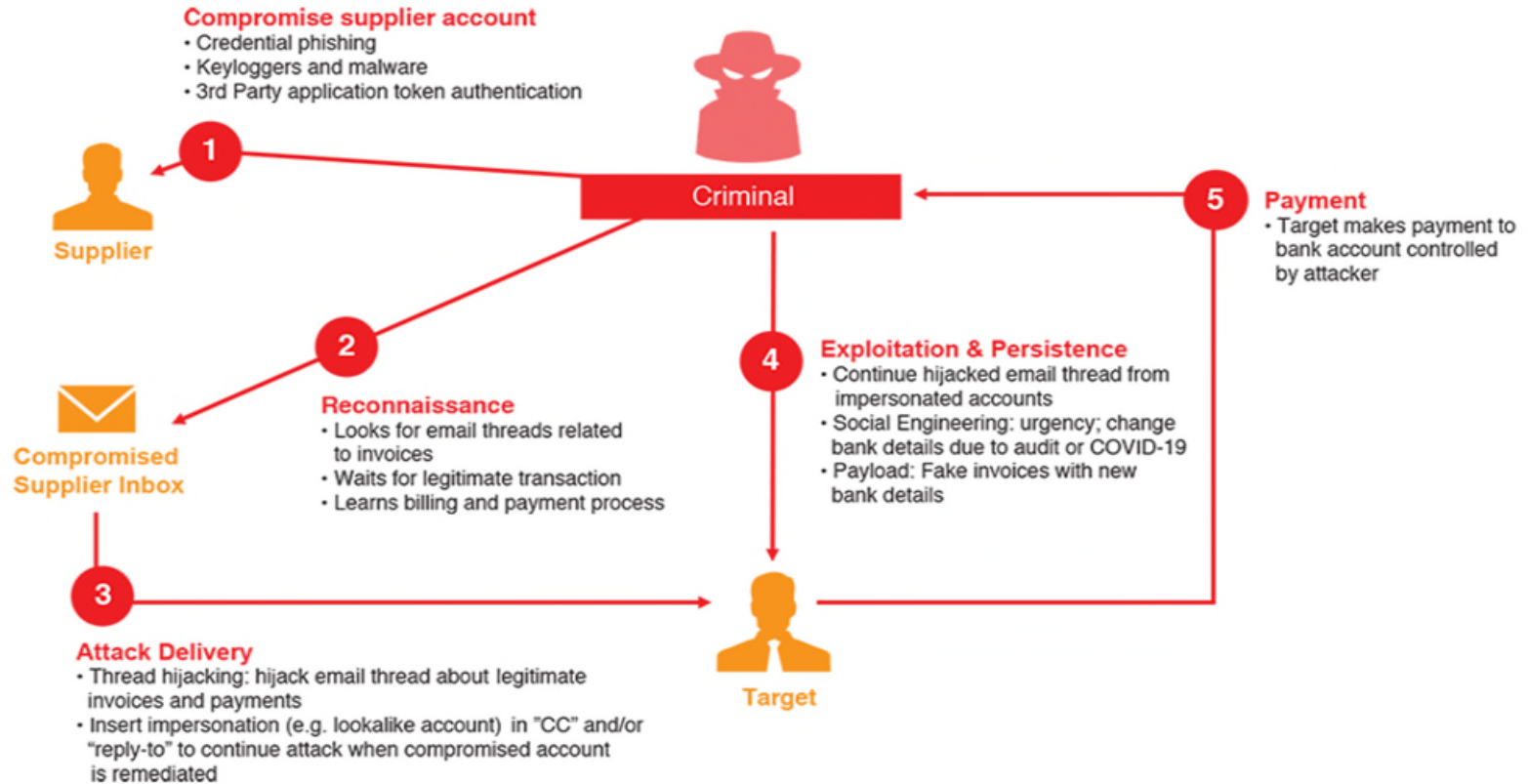


Figure 1: Anatomy of a Supplier Invoicing Fraud Attack

The threat landscape – RAT/Ransom Attack

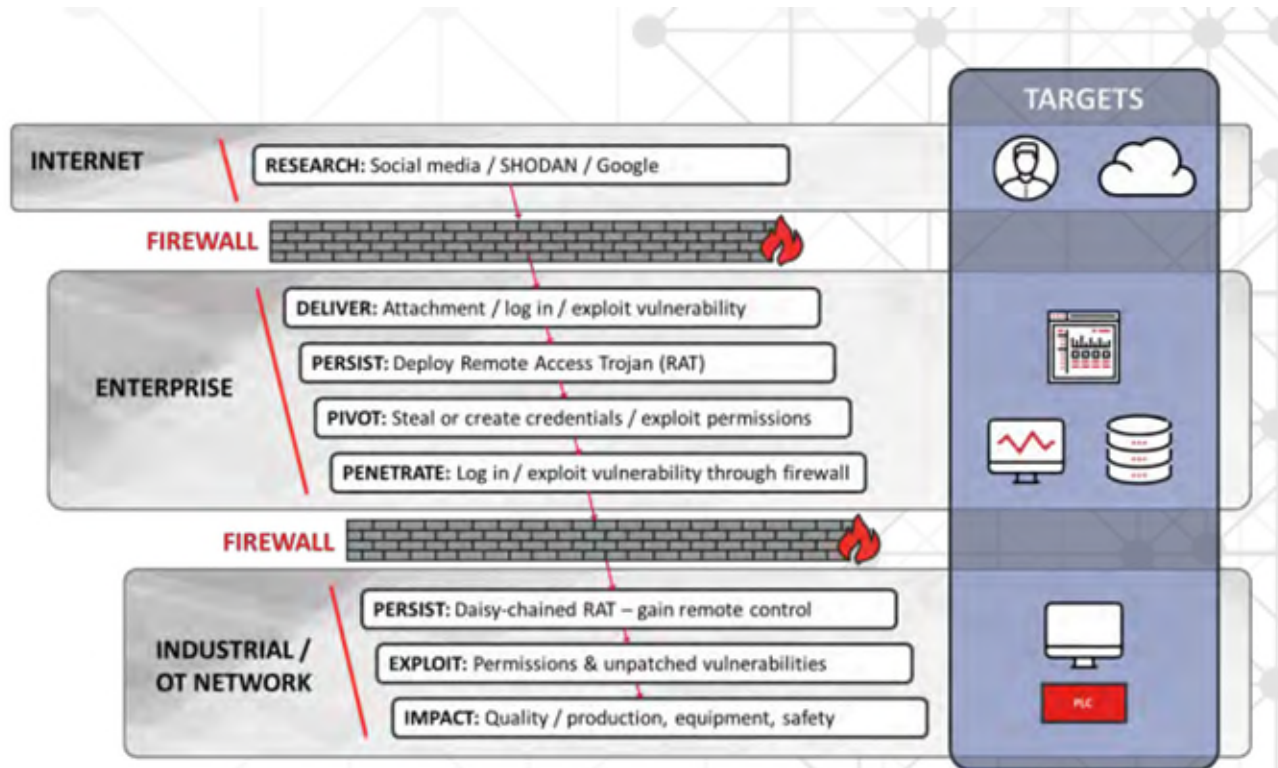


Figure (2) Manufacturing Attack Kill Chain

The law: Compliance vs Protection

NY Cybersecurity Regulation

California Consumer Privacy Protection Act

23 NYCRR 500.11

PCI-DSS

FERPA

MG 193H

COPPA

Conn. Gen. Stat. § 42-471 Regulation SP **GLBA**

HIPAA · HITECH · OMNIBUS RULE

TCPA

S.C. Insurance Data Security Law

National Assoc. of Insurance Commissioners

MODEL CYBER LAW

GDPR

C M I A

PIPEDA

The law: Compliance vs Protection

Most laws are privacy-focused not data security

The law: Compliance vs Protection

The impact of neglected data security legal obligations are felt at the worst possible moment:
after a breach has occurred

The law: Compliance vs Protection

Absence or insufficiency of data security program drives liability and cost

The law: Compliance vs Protection

Data Security Program – standards and controls:

1. Data Categorization and Management.
2. Asset Management
3. Access Controls; Monitoring
4. Vulnerability Testing
5. Third Party Oversight
6. Incident Response and Management
7. Workforce Member Training and Adherence
8. Data Retention and Destruction
9. Business Continuity and Disaster Recovery

The law: Compliance vs Protection

Scale and flexibility are key to cost effective compliance:

4. STANDARDS AND CONTROLS.

Using the results of their respective risk assessments, each assigned executive will adopt and implement Standards and Controls scaled appropriately to ensure that, at a minimum, **the most likely to occur and greatest adverse impact risks are addressed** where "Standards" means broad statements of criteria or goals to be met in order to facilitate, in a certain domain, risk:

- = reduction;
- = prevention;
- = detection; and
- = mitigation/remediation.

Standards are also sometimes referred to as "objectives" in the data security and privacy context. In turn, "Controls" are the measures designed to satisfy the stated Standard. Controls can take various forms including:

- physical;
- technical/logical;
- legal/contractual; and
- administrative.

The law: Compliance vs Protection

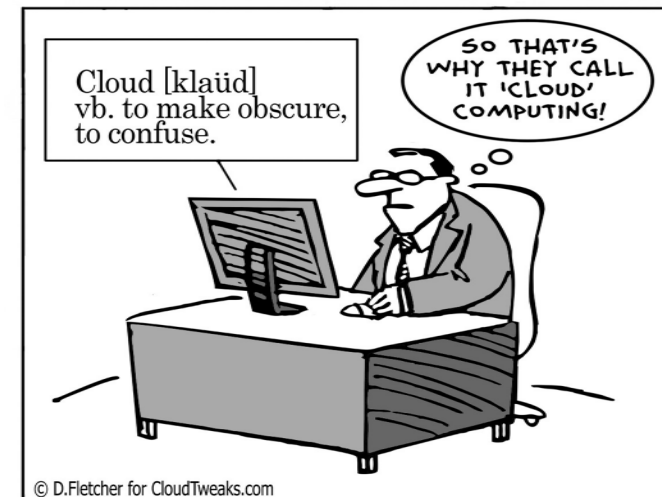
Policy compliance



Protection / Security

The law: Compliance vs Protection

Program standards and controls must be *operationalized*



Pareto Principle

80% of the results come from 20% of the effort (part 1)

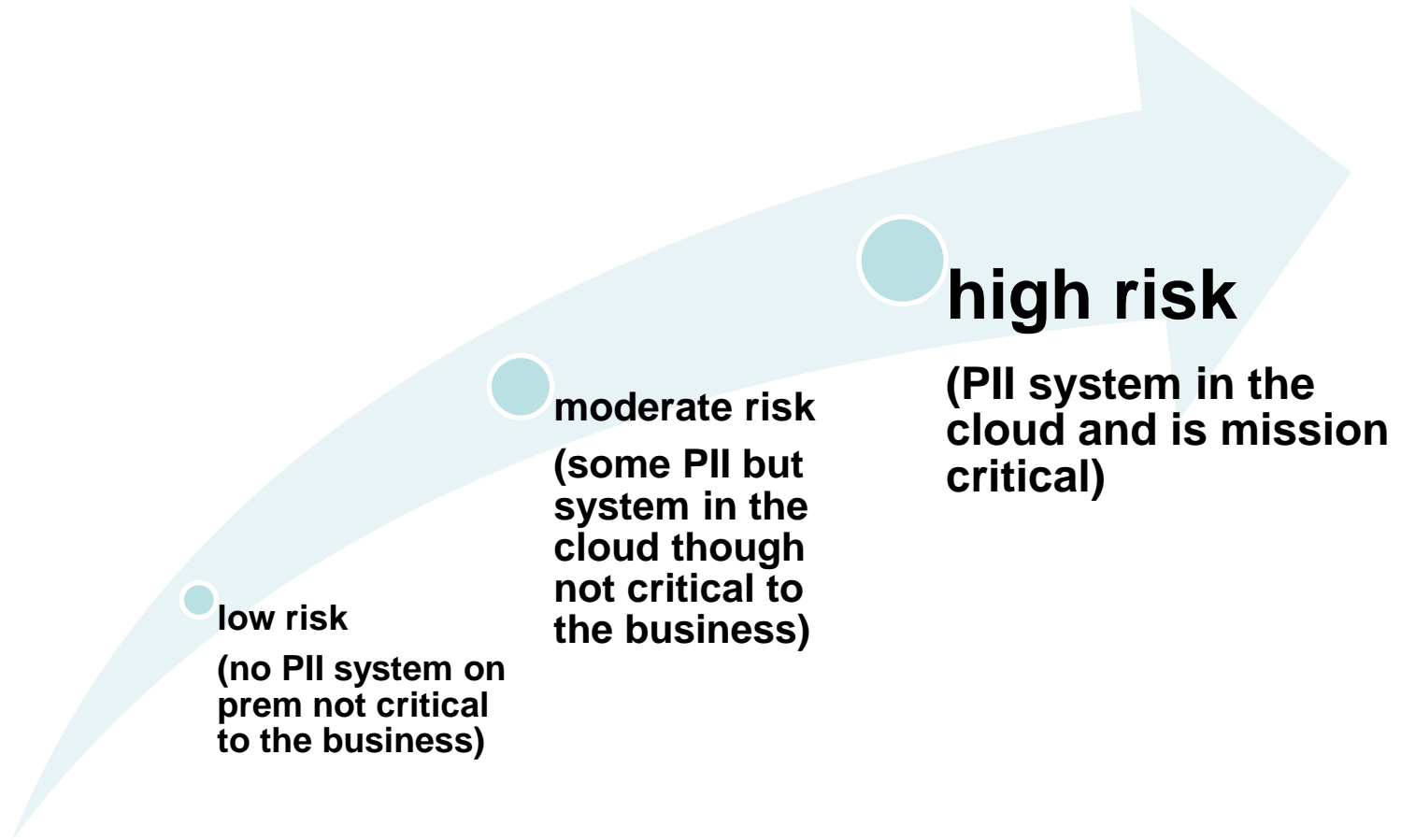
3. RISK-BASED APPROACH: RISK ASSESSMENTS.

Risk management is a key component to any successful security and privacy program. The Board therefore instructs each assigned executive and their teams to adopt a risk-based approach as it relates to identifying, adopting and implementing Standards and Controls in their assigned domain. Broadly viewed, a risk is any activity, circumstance, event or sets of events involving Company or its data that, if not remedied promptly, would be likely to have a material adverse effect on the Company's operations or reputation. Risks, as so defined, should then be viewed from two perspectives:



The Board does not require that the risk-based approach be implemented using complex quantitative methodologies. A practical, qualitative approach relying on the experience of the assigned executive is all that is necessary. Within that context, "risk likelihood" is the probability that an event giving rise to identified risk will occur. "Risk impact" is the level of adverse consequences that the Company, its Workforce Members or clients will suffer upon the actual occurrence of the event.

Pareto Principle



Pareto Principle

Keep it simple:

- Where's your data?
- Who's accessing it?
- How are they accessing it?
- What are they doing with it?
- When will it be available?
- Who will be responsible for a security incident?

Pareto Principle

80% of the results come from 20% of the effort (part 2)

1. Least privileged access
2. Encryption
3. Multi-factor Authentication*
4. End-point monitoring
5. Vendor Contracting

Reality Check

On Premises

- installed on your server
- at your facility
- license fee separate from maintenance/support fee
- substantial implementation

Hosted

- installed on your or vendor server
- at vendor facility
- hosting fee added
- hosting environment set up needed in addition to implementation

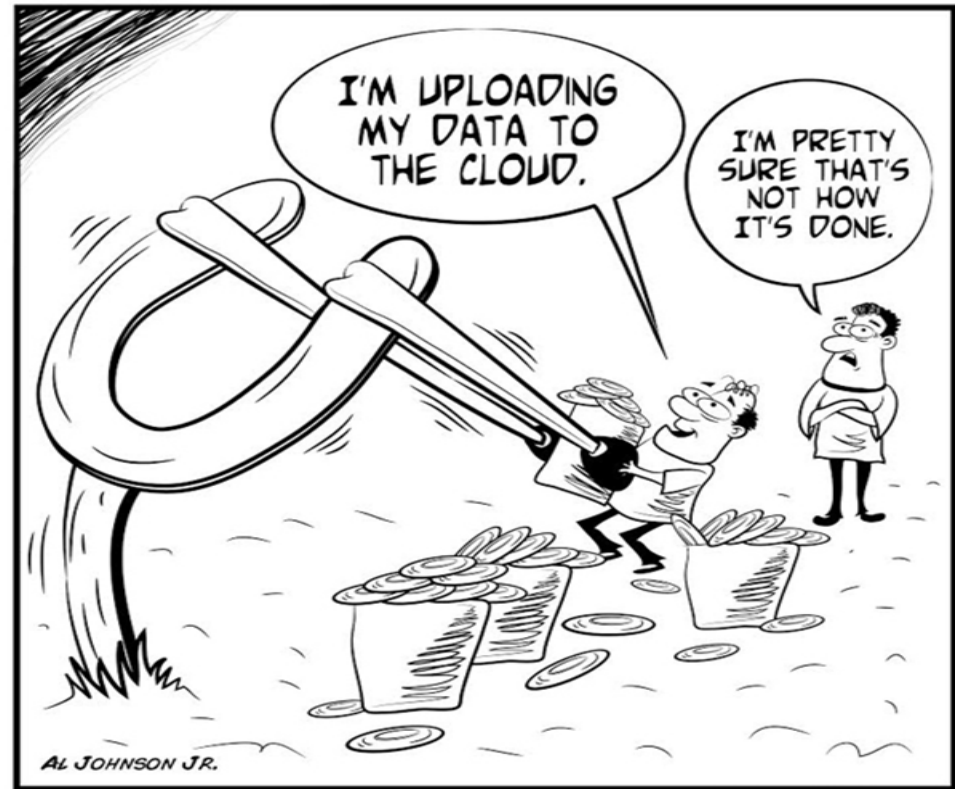
X-a-a-S

- vendor's server
- vendor's facility
- single fee
- minimal set up

a few good clauses

Where's Your Data?

- On-shore or Off?
- Facilities Quality?
- Change of Location?



© CloudTweaks.com

a few good clauses

Where's Your Data?

On-shore or Off?

In no event, whether by itself or through any otherwise approved Third Party Supplier, shall Supplier perform Services **outside the continental United States** or its commonwealths, territories and possessions (including indirectly **via remote network access**) without the prior written consent of Customer in each instance.

Change of Location?

Migration. Supplier shall provide reasonable **advance notice** of any change in any Approved Facility location with reasonable assurances that the new data center meets the requirements hereunder. Supplier shall perform, **at no additional charge** (for either fees or expenses), all such services as are necessary to complete the orderly transition of the applicable services and data to the new facilities (the “**Migration Services**”). The Migration Services shall be performed in accordance with a plan and on a schedule approved by Customer, which approval shall not be unreasonably withheld, delayed or conditioned. There shall be no suspension **or change in any service levels** during the Migration Services unless otherwise agreed in writing by the parties and a discount or waiver of fees is provided to Customer in an amount reasonably proportionate to the period of suspension or magnitude of change.

a few good clauses

Who's Accessing Your Data?

- Vendor Personnel
- Subcontractors
- Third Parties



a few good clauses

Who's Accessing Your Data?

Vendor Personnel

Supplier shall assign to Customer's account only its employees or individual subcontractors of the type commonly referred to as "1099's" ("Supplier Personnel"). All other personnel providing Services shall be considered third party subcontractors and governed by the Third Party Supplier provisions of Section 6.6. All Supplier Personnel, and the personnel of all permitted Third Party Suppliers, shall be screened for: (a) convictions of felonies and financial-related crimes committed during the last seven years; (b) verification they are not subject to or included on the regulations administered by the Office of Foreign Assets Control of the United States Department of the Treasury through the General Services Administration's Federal Acquisition Regulation compliance program; and (c) compliance with immigration laws.

a few good clauses

Who's Accessing Your Data?

Subcontractors

Supplier shall not, without the prior written consent of Customer, provide the Services through any third party including any Supplier Affiliates (each a “Third Party Supplier”). If Customer approves Supplier’s use of a Third Party Supplier: (a) Supplier shall be the prime contractor to Customer with respect to such Third Party Supplier and shall assume full responsibility and liability for the Services and acts and omissions of the Third Party Supplier (including any liens or encumbrances Third Party Supplier’s place or purport to assert on Customer property); and (b) prior to disclosing any of Customer’s Confidential Information (defined in Article 9) or performance of Services by such Third Party Supplier, Supplier shall have entered into a written agreement with the Third Party Supplier expressly binding such Third Party Supplier **to the confidentiality and data security provisions.** IPR (defined in Section 7.8(b)) provisions and such other terms of this Agreement as Customer may require and such terms and conditions shall govern irrespective of any contrary term or condition that may be contained in a separate agreement between Supplier and a Third Party Supplier. At Customer’s request, Supplier shall provide Customer with written evidence in a form reasonably acceptable to Customer of compliance with the foregoing.

a few good clauses

Who's Accessing Your Data?

Non-Subcontractor Third Parties

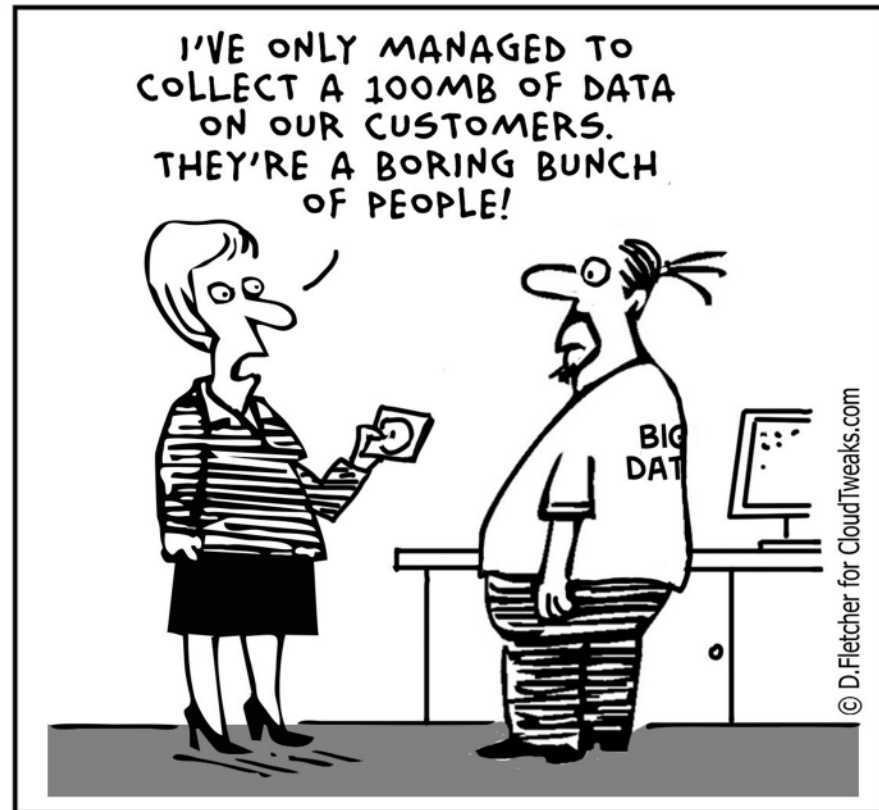
Facilities Standards – SOC 2 and ISO 2700x

- dual-factor access control (with at least one biometric factor) at principal facility access points
- single-factor biometric authentication to all interior secure areas
- single-factor biometric access control at individual cage access points
- 24x7x365 on-site security, CCTV surveillance of interior and exterior strategic locations and access points with a minimum of 10 days video retention

a few good clauses

What are they doing with your Data?

- Restricting Use
- Allowing Aggregation



a few good clauses

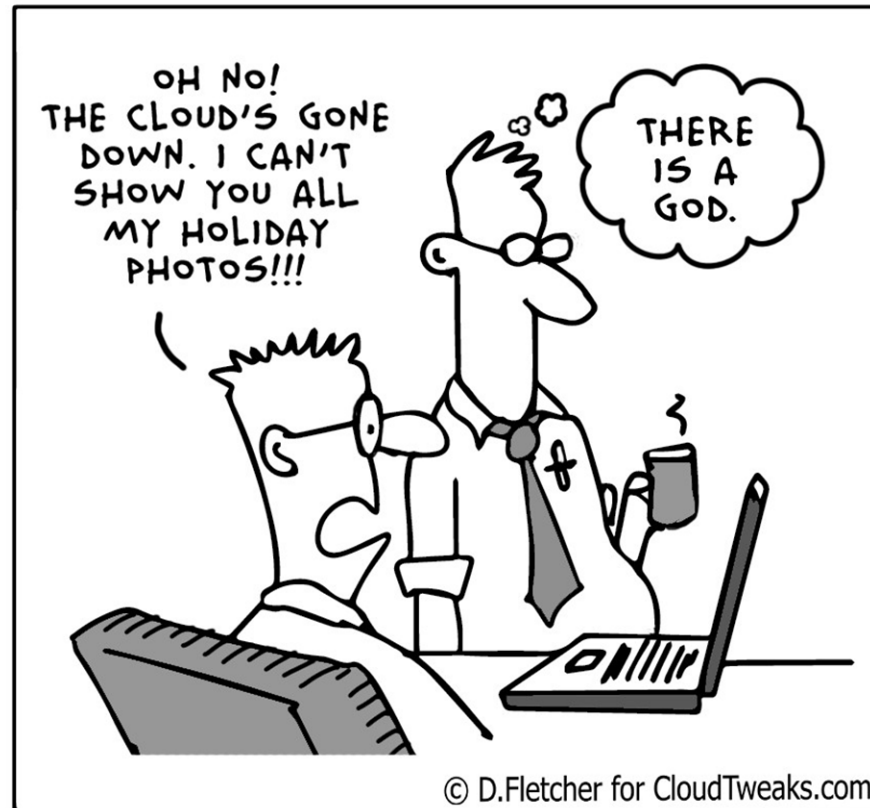
What are they doing with it?

As between Supplier and Customer, all data provided to Supplier by or on behalf of Customer and/or its Affiliates under this Agreement (“Customer Data”), remains the sole property of Customer. Those elements of Customer Data recognized at law as trade secrets shall be governed by Customer’s ownership of IPR above. All Customer Data, whether or not trade secret, shall be Customer’s Confidential Information, subject to the terms of this Agreement. Additional terms with respect to certain types of Customer Data are set forth in Article 9 hereto. Unless otherwise agreed by the parties in writing, only Supplier Personnel located within the United States and its territories, commonwealths, and possessions will have access to Customer Data. Supplier Personnel shall not have the right to copy Customer Data except to the limited extent necessary to perform under this Agreement. Supplier shall be responsible for deletion, destruction, or alteration of Customer Data while in the possession or custody or under the control of Supplier Personnel. Customer Data shall not be used by Supplier for any purpose other than that of providing Services, nor shall Customer Data be disclosed, sold, assigned, leased, or otherwise disposed of to third parties by Supplier, or commercially exploited by or on behalf of Supplier and Supplier Personnel. Upon Customer’s request at any time during the Master Term, Supplier shall deliver all Customer Data then being maintained by Supplier in such form or media as is reasonably requested by Customer.

a few good clauses

When will your data be available?

- Uptime SLA
- Periodic Delivery
- Post-Termination



a few good clauses

When will your data be available?

Uptime SLA – the basics

Without limiting Supplier's obligations to meet the Availability Service Level (defined below), Supplier shall use commercially reasonable efforts to make sure that the Software and portions thereof will be "available" to Authorized Users **24 hours per day, 7 days per week, 365 days per year.** Notwithstanding the foregoing, Supplier shall ensure that the Software is "available" for use by Authorized Users ninety-nine and nine tenths percent **(99.9%)** of the time 7 days per week, 365 days per year excluding Scheduled Downtime (the "**Availability Service Level**"). For purposes of this Agreement, System "available" and its variants means a working database server with the Software and Customer's database(s) mounted, running, and accessible from all servers to the public Internet. **"Scheduled Downtime"** means 6:00 p.m. Saturday Eastern prevailing time through 5 a.m. Monday Eastern prevailing time.

a few good clauses

When will your data be available?

Uptime SLA – tricks of the trade

Supplier will be responsible for the hardware, equipment, telecommunications and networking infrastructure necessary to provide the Software from a point of demarcation starting with the Appliance permitting ingress to the Data Center from the WAN Circuit, continuing thereafter to the Data Center's egress Appliance back to the Public Circuit. For avoidance of doubt, Supplier is not responsible for the Public Circuit itself, except that Supplier shall perform an industry-accepted ping-like monitoring test of the telecommunications line connected to its ingress/egress Appliance every ten (10) minutes and immediately take corrective action if such test does not return a signal indicating proper functioning. As used herein the term "**Appliance**" means either a router, or if a dedicated PBX or switching software is leased or owned by Supplier, such PBX or switching software; and where the term "**Public Circuit**" means the third party provided circuits, overland and/or submarine cabling and other connectivity infrastructure from a point of demarcation starting at the point immediately after the ingress/egress Appliance at the Customer site to the point immediately before the ingress/egress Appliance router at the Data Centers.

a few good clauses

When will your data be available?

Periodic Delivery

Data Refreshes; Backup and Data Return. On a continuous basis, Supplier shall refresh Customer Data transmitted through the Software provided by Customer's Authorized Users. Upon Customer's written request from time to time (but no more than once per quarter), Supplier shall provide to Customer a copy of all of Customer Data provided by Customer's Authorized Users in a format mutually agreed to by the parties. Unless more frequent back-ups are provided under Supplier's separate back-up and DR-BC Plan, back-up services shall be performed for all Customer Data at least daily with offsite storage of all media used therefor.

a few good clauses

When will your data be available?

Post-Termination

The Disengagement Services shall include the performance by Supplier of such services as shall be necessary to facilitate the orderly transfer of the Client Data to Client or its designee including delivery of Client Data in native or other agreed format which shall in all events be readable/useable with common, commercially available software. Supplier shall have no right to delete Client Data from its servers until 180 days after termination or expiration or 10 days following completion of the agreed Disengagement Services, whichever is later. At that time, Supplier shall certify to such destruction in writing.

a few good clauses

What if there's a disaster?

- The Basic Plan
- The SLAs
- Force Majeure



a few good clauses

What if there's a disaster?

The Basic Plan

Supplier has established, tested and throughout the Master Term, will maintain and test at least annually, for each facility from which, and all elements of infrastructure on which, the Services are provided and/or Software deployed, a comprehensive disaster recovery and business continuity plan (the "DRBC Plan") sufficient to respond to and manage any event, whether or not within Supplier's control, that is or may reasonably be expected to prevent or materially adversely affect Supplier's performance, or damage Supplier facilities, infrastructure or assets including the loss of production, systems or equipment, supply chain failures, failure of carriers and the failure of Supplier's equipment, computer systems or business systems (in all cases including both short and long term disruptions) ("DRBC Events"). Consistent with industry standards and best practices, the DRBC Plan shall at a minimum, include a recovery strategy and appropriate procedures to resume the Services within no more than 72 hours of the occurrence of the DRBC Event and no greater than 24 hours of data loss. Upon Customer's request, Supplier will: (i) certify the DRBC Plan is fully operational and continues to be tested no less than once annually; (ii) provide Customer with a copy of the DRBC Plan and/or any results of the test thereon; and (iii) permit Customer (or its designated third party auditor, subject to confidentiality restrictions) to observe annual testing of the DRBC Plan. Supplier shall immediately implement the DRBC Plan upon the occurrence of a DRBC Event and, notwithstanding anything to the contrary herein, will not be relieved from such obligation on account of an FM Event. The reinstatement of the Services (or availability of the Software) under the affected Agreements will receive as high or greater priority as that of reinstatement of services for Supplier's Affiliates and other customers.

a few good clauses

What if there's a disaster?

The SLAs – RTO and RPO

Supplier has established, tested and throughout the Master Term, will maintain and test at least annually, for each facility from which, and all elements of infrastructure on which, the Services are provided and/or Software deployed, a comprehensive disaster recovery and business continuity plan (the “DRBC Plan”) sufficient to respond to and manage any event, whether or not within Supplier’s control, that is or may reasonably be expected to prevent or materially adversely affect Supplier’s performance, or damage Supplier facilities, infrastructure or assets including the loss of production, systems or equipment, supply chain failures, failure of carriers and the failure of Supplier’s equipment, computer systems or business systems (in all cases including both short and long term disruptions) (“DRBC Events”). Consistent with industry standards and best practices, the DRBC Plan shall at a minimum, include a recovery strategy and appropriate procedures to resume the Services within no more than 72 hours of the occurrence of the DRBC Event and no greater than 24 hours of data loss.

Upon Customer’s request, Supplier will: (i) certify the DRBC Plan is fully operational and continues to be tested no less than once annually; (ii) provide Customer with a copy of the DRBC Plan and/or any results of the test thereof; and (iii) permit Customer (or its designated third party auditor, subject to confidentiality restrictions) to observe annual testing of the DRBC Plan. Supplier shall immediately implement the DRBC Plan upon the occurrence of a DRBC Event and, notwithstanding anything to the contrary herein, will not be relieved from such obligation on account of an FM Event. The reinstatement of the Services (or availability of the Software) under the affected Agreements will receive as high or greater priority as that of reinstatement of services for Supplier’s Affiliates and other customers.

a few good clauses

What if there's a disaster?

Force Majeure

Neither party shall be deemed in default or otherwise liable for any delay in or failure of its performance under this Agreement by reason of any act of God, act of war or terrorism, fire, natural disaster, accident, riot, act of government or third party strike or labor dispute (each, an "FM Event"); provided however, that: (i) the party suffering from such FM Event shall provide the other party with written notice immediately upon becoming actually aware of its occurrence; (ii) in addition to any other remedy at law, in equity or under this Agreement, the other party may terminate an affected Agreement, and in the case of Customer, receive a pro-rata refund of any prepaid amounts remaining as unearned as of the time of termination if performance is not re-commenced within 10 calendar days of the occurrence of the FM Event; and (iii) nothing herein shall relieve Supplier of any disaster recovery or business continuity obligations under an Order. For avoidance of doubt, unless an FM Event substantially frustrates all material performance obligations despite diligent efforts, such event shall not operate to excuse, but only to delay, performance.

a few good clauses

Who's responsible for security incidents?

- Notice and Response
- Remedies
- Liability



a few good clauses

Who's responsible for security incidents?

Notice and Response

Immediately upon becoming aware of a Security Breach, Data Handler shall activate and implement the incident response and management elements of the Security Program as set forth in Section 4.1 above. In addition, Data Handler shall: (a) provide Company with written notice within 24 hours of Data Handler becoming aware of the Security Breach; (b) preserve all information and evidence related to the Security Breach (including by suspending routine overwriting or deletion of data or log files); and (c) allow Company to reasonably participate in the investigation of the Security Breach and/or conduct its own parallel independent investigation (including by making servers, storage devices and media available to Company, or its designated representative, for forensic imaging and analysis). In all events, Data Handler shall, at Data Handler's cost, retain as a Permitted Subcontractor hereunder, an independent forensic investigator to image and preserve the affected hardware and equipment, to investigate the scope and cause of the Security Breach (including, which data fields were compromised and the individuals affected by such compromise) and to minimize the effects of the Security Breach, including steps to secure Company Data. In such case, Data Handler agrees (so long as permitted by law/law enforcement) to permit the forensic investigator to disclose any information and evidence to Company related to cause, scope, and extent of the Security Breach. Data Handler shall not charge Company for the cost of any work to be performed in connection with the investigation or remediation. Except as may be required by applicable law, Data Handler agrees that it will not disclose the occurrence of a Security Breach to any third party, including any governmental or industry self-regulatory authority, without first obtaining Company's prior written consent.

a few good clauses

Who's responsible for security incidents?

Remedies

To the extent a Security Event triggers an obligation under the Data Handling Rules to provide: (a) notification to public authorities or regulators, such as the Attorneys General of the several United States, the New York State Superintendent of Financial Services, the Office of Civil Rights within the U.S. Department Health and Human Services or any Data Protection Authority in the Swiss Confederation or any EU member nation; (b) notification to individuals whose Personal Data is included in the Company Data; or (c) undertake remedial measures such as providing credit monitoring services, identity theft insurance or the like (each of the foregoing, a "Remedial Action"), at Company's request.

Data Handler shall, at Data Handler's cost, undertake Remedial Actions and, in any event, will remain financially responsible therefor whether such Remedial Actions are undertaken by Data Handler or Company. The timing, content, and manner of effectuating such Remedial Action shall be agreed by the parties and in all cases shall comply with the applicable Data Handling Rules.

a few good clauses

Who's responsible for security incidents?

Liability

- Fully indemnified
- Uncapped
- Inclusive of consequential damages
- Ipso facto

GORDON&REES

SCULLY MANSUKHANI

www.grsm.com