Preparing For Cyber Attack

‘Risk’ is defined as the likelihood of loss. Assessing cyber risk entails estimating the likelihood of an organization experiencing different levels and types of loss.

These can be broken down into a number of key loss processes, for example:

- Data exfiltration
- Contagious malware attacks
- Denial of service attacks
- Financial transaction theft
- Failures of counterparties or suppliers

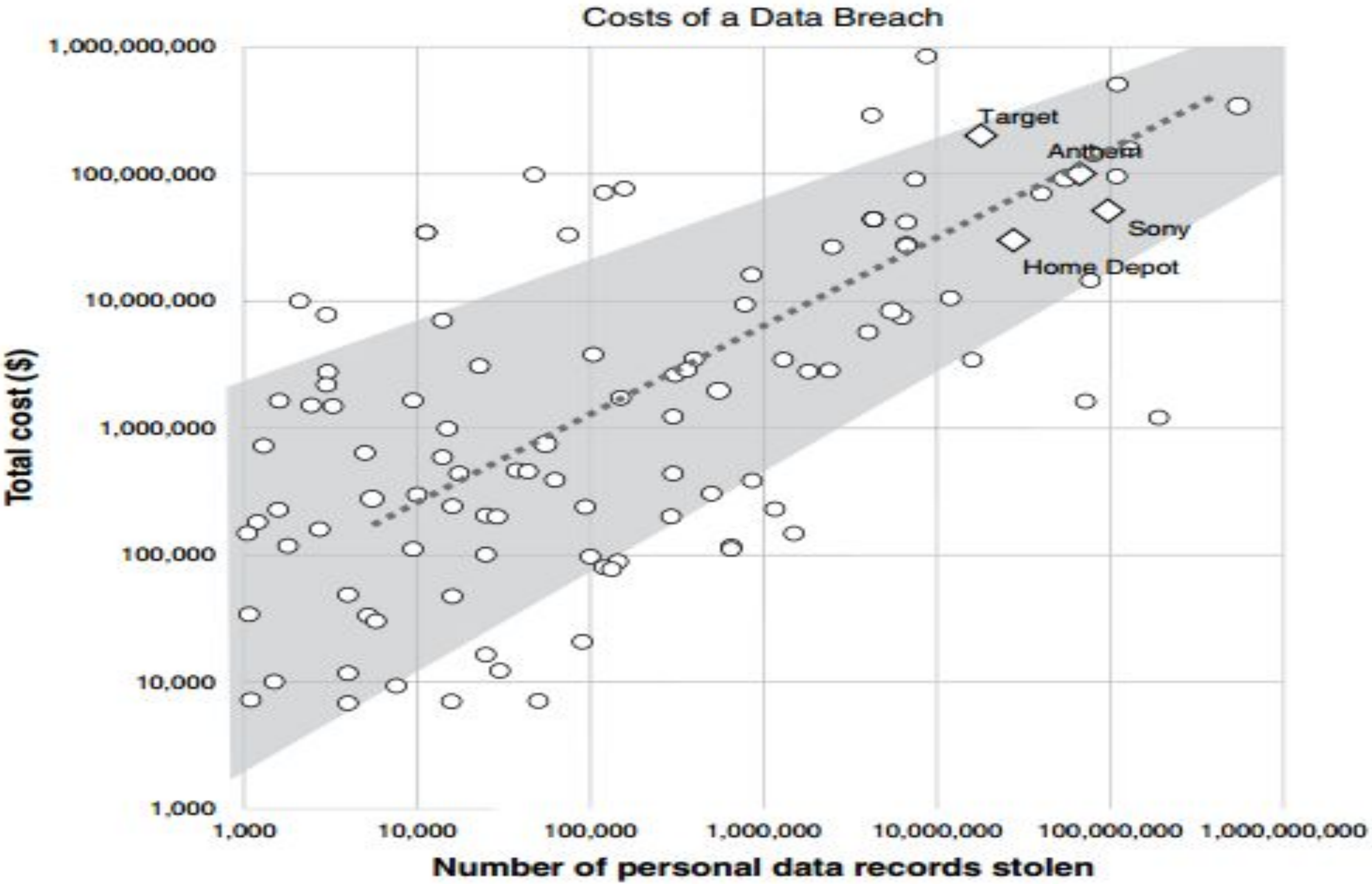


FIGURE 2.1 Costs of US data breaches by size of breach (2012–2017).

DATA EXFILTRATION

Target Corporation: the loss of confidential data from companies that breach the privacy of their customers, employees, clients, or counterparties. If these fall into the wrong hands, they may reveal sensitive financial information about the business, intellectual property that provides competitive advantages to rivals, or information that can be publicized to damage the reputation of the company. wrong hands can be used for identity theft, to conduct fraudulent transactions, to steal money from bank accounts, to blackmail or demand ransom from the individual, or for other activities that are harmful to the data owner.

Protecting your Data

Many companies now operate procedures to protect their data, and it is common in larger companies to use a sensitive data management system to identify internal data, track its usage, and control the access to it.

The regulatory requirement for organizations to notify the loss of personal confidential data has been in place longest in the United States, where it has been a requirement in most states since 2002. Since then there have been many thousands of notified events. The number of reported events grew very rapidly after 2009, but peaked in the years 2013 to 2016, and has been at a similar level or less in subsequent years.

- Data exfiltration occurs through accidental loss, insider exfiltration, or malicious external action. Before around 2010, two-thirds of incidents where data was compromised was through accidents – typically unsecured laptops or unencrypted data media being lost.

- There has been a rapid increase in malicious external attacks to steal data, until it has become the cause of three-quarters of data exfiltration incidents.

- Insider threat – or whistle-blowing – became more common for a few years after 2010, accounting for around 20% of leaks in 2012, but reducing back to around the previous rate of 10% of events from around 2014 onwards.

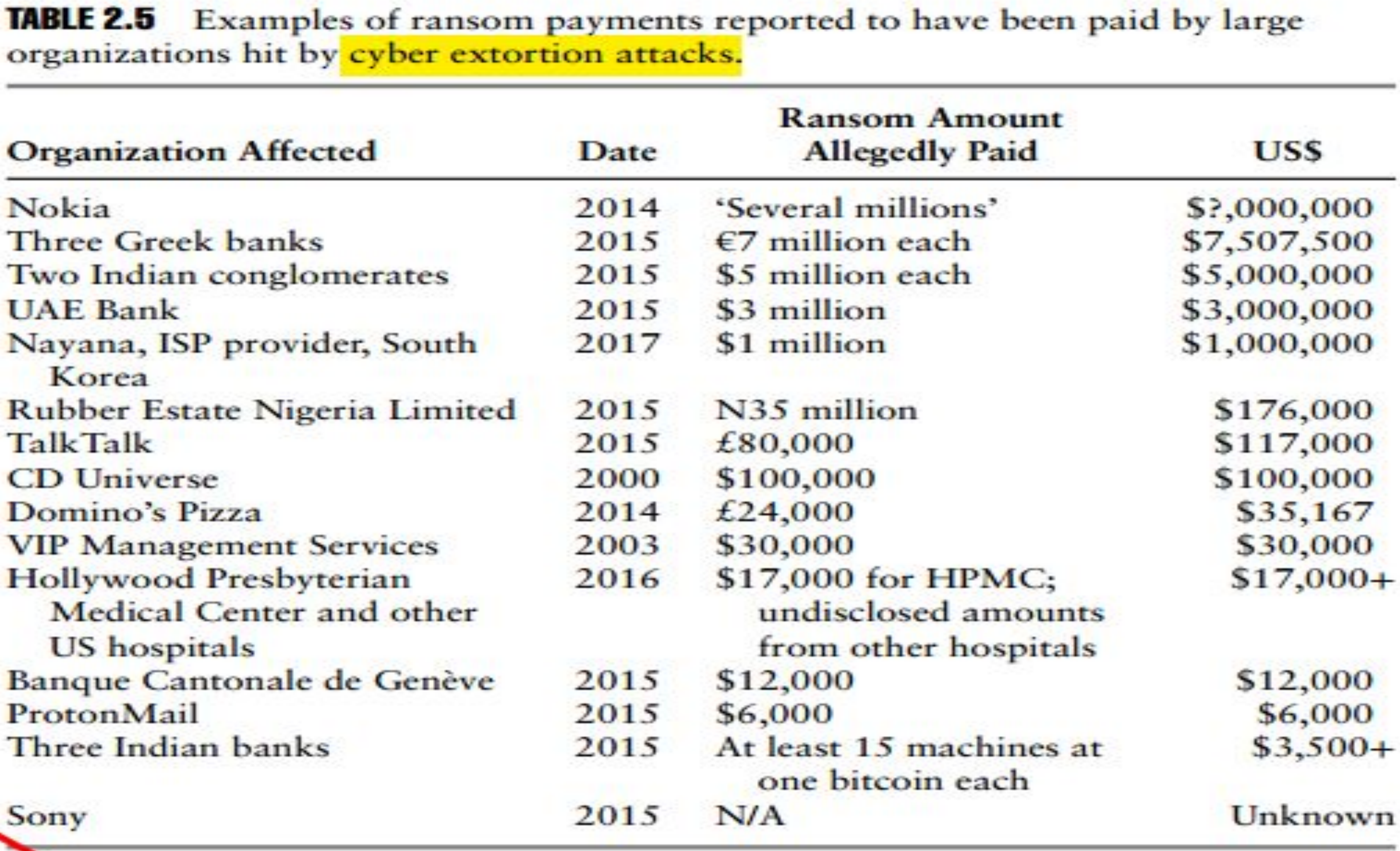
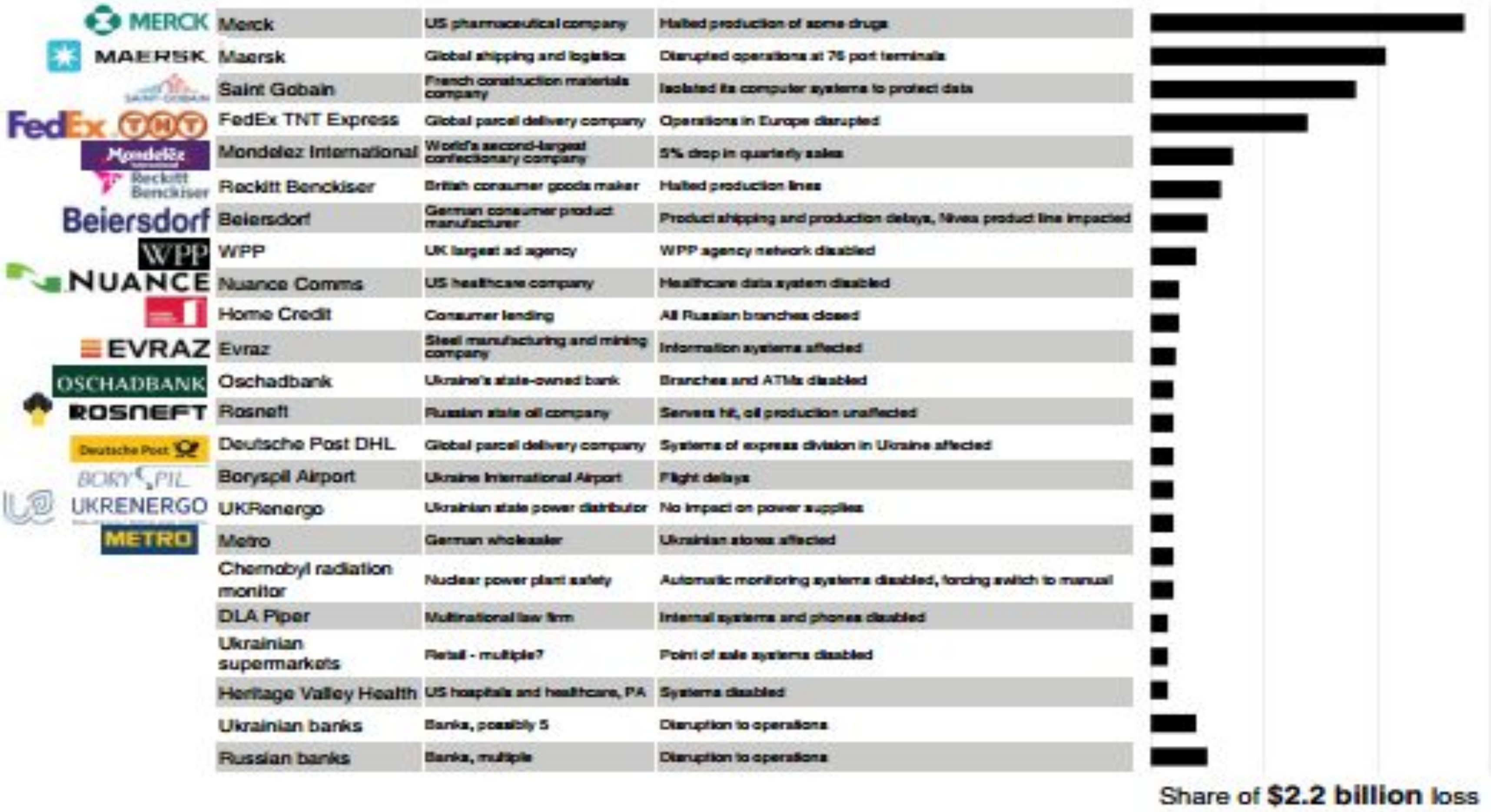


TABLE 2.5 Examples of ransom payments reported to have been paid by large organizations hit by cyber extortion attacks.

Organization Affected	Date	Ransom Amount Allegedly Paid	US$
Nokia	2014	'Several millions'	$?,000,000
Three Greek banks	2015	€7 million each	$7,507,500
Two Indian conglomerates	2015	$5 million each	$5,000,000
UAE Bank	2015	$3 million	$3,000,000
Nayana, ISP provider, South Korea	2017	$1 million	$1,000,000
Rubber Estate Nigeria Limited	2015	N35 million	$176,000
TalkTalk	2015	£80,000	$117,000
CD Universe	2000	$100,000	$100,000
Domino's Pizza	2014	£24,000	$35,167
VIP Management Services	2003	$30,000	$30,000
Hollywood Presbyterian Medical Center and other US hospitals	2016	$17,000 for HPMC; undisclosed amounts from other hospitals	$17,000+
Banque Cantonale de Genève	2015	$12,000	$12,000
ProtonMail	2015	$6,000	$6,000
Three Indian banks	2015	At least 15 machines at one bitcoin each	$3,500+
Sony	2015	N/A	Unknown



Merck	US pharmaceutical company	Halted production of some drugs
Maersk	Global shipping and logistics	Disrupted operations at 76 port terminals
Saint Gobain	French construction materials company	Isolated its computer systems to protect data
FedEx TNT Express	Global parcel delivery company	Operations in Europe disrupted
Mondelez International	World's second-largest confectionary company	5% drop in quarterly sales
Reckitt Benckiser	British consumer goods maker	Halted production lines
Beiersdorf	German consumer product manufacturer	Product shipping and production delays, Nivea product line impacted
WPP	UK largest ad agency	WPP agency network disabled
Nuance Comms	US healthcare company	Healthcare data system disabled
Home Credit	Consumer lending	All Russian branches closed
Evraz	Steel manufacturing and mining company	Information systems affected
Oschadbank	Ukraine's state-owned bank	Branches and ATMs disabled
Rosneft	Russian state oil company	Servers hit, oil production unaffected
Deutsche Post DHL	Global parcel delivery company	Systems of express division in Ukraine affected
Boryspil Airport	Ukraine International Airport	Flight delays
UKRenergo	Ukrainian state power distributor	No impact on power supplies
Metro	German wholesaler	Ukrainian stores affected
Chernobyl radiation monitor	Nuclear power plant safety	Automatic monitoring systems disabled, forcing switch to manual
DLA Piper	Multinational law firm	Internal systems and phones disabled
Ukrainian supermarkets	Retail - multiple?	Point of sale systems disabled
Heritage Valley Health	US hospitals and healthcare, PA	Systems disabled
Ukrainian banks	Banks, possibly 5	Disruption to operations
Russian banks	Banks, multiple	Disruption to operations

FIGURE 2.3 Examples of losses caused to businesses by *NotPetya* malware, June 2017.

Costs of Data Exfiltration

- The company may need to handle large numbers of enquiries from concerned people who want to know if they have been affected. Individuals who have had their personal data compromised are entitled to credit monitoring services for a period of time in case they suffer identity theft.
- Regulators typically impose fines on the company for its failure in the duty of trust. The organization also faces internal costs from dealing with the breach, including a forensic investigation to identify and rectify any IT system vulnerability that was the cause of the breach, installation of higher levels of security, and disruption to its business practice while it deals with the immediate aftermath of the event.

- The type of data stolen is important: for a breach of 10,000 records, it will cost a company 1.5 times as much for PCI records than for personally identifiable information (PII), and 5.5 times as much for protected health information (PHI) records.

- The average cost per record of a data loss of more than 100,000 records more than doubled from 2010 to 2016.2 This reflects increasing regulatory fines and procedures, growing costs of compensation, and escalation of legal complexities in dealing with identity loss

TABLE 2.3 Examples of contagious malware outbreaks ranked by global impact, past 30 years.

Name	Global Impact	Year	Type	Propagation Vector	Infection Rate	Payload Type	Destructiveness
Conficker	1: Very high	2008	Worm	IP block scanning	1: Very high	Botnet	1: Very high
ILOVEYOU	1: Very high	2000	Worm	Email	1: Very high	Overwriting files	1: Very high
MyDoom	1: Very high	2004	Worm	Email	2: High	DDoS	1: Very high
Netsky	1: Very high	2004	Worm	Email	3: Moderate	Beeping	1: Very high
Sasser	1: Very high	2004	Worm	Buffer overflow	3: Moderate	DDoS	1: Very high
NotPetya	2: High	2017	Virus	Software update	3: Moderate	Wiper	2: High
WannaCry	2: High	2017	Worm	Random scanning	2: High	Ransomware	2: High
Stuxnet	2: High	2010	Worm	Search (Siemens software)	4: Significant	SCADA control	1: Very high
SQL Slammer	2: High	2003	Worm	Buffer overflow	1: Very high	DDoS	2: High
Mirai	2: High	2016	Worm	WAN scanning	1: Very high	Botnet	3: Moderate
Klez	2: High	2001	Worm	Email	3: Moderate	HTML message	1: Very high
Code Red	2: High	2001	Worm	Buffer overflow	3: Moderate	Website defacing, DDoS	2: High
Melissa	2: High	1999	Virus	Email	3: Moderate	Spam generator	4: Significant
Nimda	2: High	2001	Worm	Email + web browser	4: Significant	Ransomware	2: High
Sality	3: Moderate	2003	Virus	Email	1: Very high	Keystroke logging	2: High
Chernobyl	3: Moderate	1998	Virus	Pirated software	2: High	Overwriting files	3: Moderate
Morris	3: Moderate	1988	Worm	Multiplatform (inc. email)	2: High	Botnet	5: Material
Shamoon	3: Moderate	2012	Virus	Spear phishing	2: High	Wiper	2: High
Blaster	3: Moderate	2003	Worm	Random scanning	3: Moderate	Botnet	2: High
Bad Rabbit	3: Moderate	2017	Worm	Corrupted software	3: Moderate	Ransomware	2: High

Neverquest	3: Moderate	2013	Trojan	Email, web injection	3: Moderate	Botnet	3: Moderate
Zeus	3: Moderate	2007	Trojan	Software download	3: Moderate	Keyloggers/HTML injectors	4: Significant
CoinMiner	3: Moderate	2018	Virus	Random scanning	3: Moderate	Cryptocurrency miner	5: Material
Locky	3: Moderate	2016	Virus	Email	4: Significant	Ransomware	3: Moderate
Tiny Banker	4: Significant	2012	Trojan	Email	4: Significant	Packet sniffing	1: Very high
KOVTER	4: Significant	2017	Virus	Email	4: Significant	Click fraud	2: High
ONI/MBR-ONI	4: Significant	2017	Virus	Email	4: Significant	Wiper	2: High
Dukakis	4: Significant	1988	Virus	Floppy disk	5: Material	Displays a message	5: Material
SevenDust	4: Significant	1998	Virus	Email	5: Material	Wiper	2: High
FakeAV	5: Material	2007	Trojan	Corrupting software, email	3: Moderate	Scareware	4: Significant
Storm	5: Material	2007	Trojan	Email	3: Moderate	Botnet	4: Significant
Magic Lantern	5: Material	2001	Trojan	Email	5: Material	Keystroke logging	5: Material
Michelangelo	5: Material	1991	Trojan	Driver disks	5: Material	Data destruction	3: Moderate

Virus

‘virus’ –computer code inside a host program; ‘worm’ – a stand-alone piece of compiled software as a program that can replicate itself; and ‘Trojan horse’ – a program that appears to do one thing but actually does something different.

Wanna Cry

- May 12, 2017 when an aggressive ransomware attack via file-sharing network protocols on computers using outdated Windows XP and v8 OS resulted in 300,000 infections of computers across 150 countries. The WannaCryptor used a National Security Agency (NSA) exploit code-named EternalBlue.
- Of the roughly 400 million actively used Windows computers running version 8 or an earlier operating system, approximately 0.1% were infected.
- The event highlighted the issue of equipment software latency, i.e. that machines and subnetworks within organizations may rely on specific versions of an operating system that render them vulnerable.

- Machines such as medical magnetic resonance imaging (MRI) scanners and X-ray machines that were certified only on XP and v8, and maintained on those operating systems, were among those that were crippled by the attack.
- Estimates of the losses caused by WannaCry vary substantially, from tens of millions of dollars to $4 billion.
- Our counterfactual analysis suggests that if the kill switch had not been triggered, and if the attack had occurred prior to the issuing of the MS17-010 patch for Windows 8, the infection rates and losses could have been an order of magnitude higher, perhaps reaching $20 billion to $40 billion.

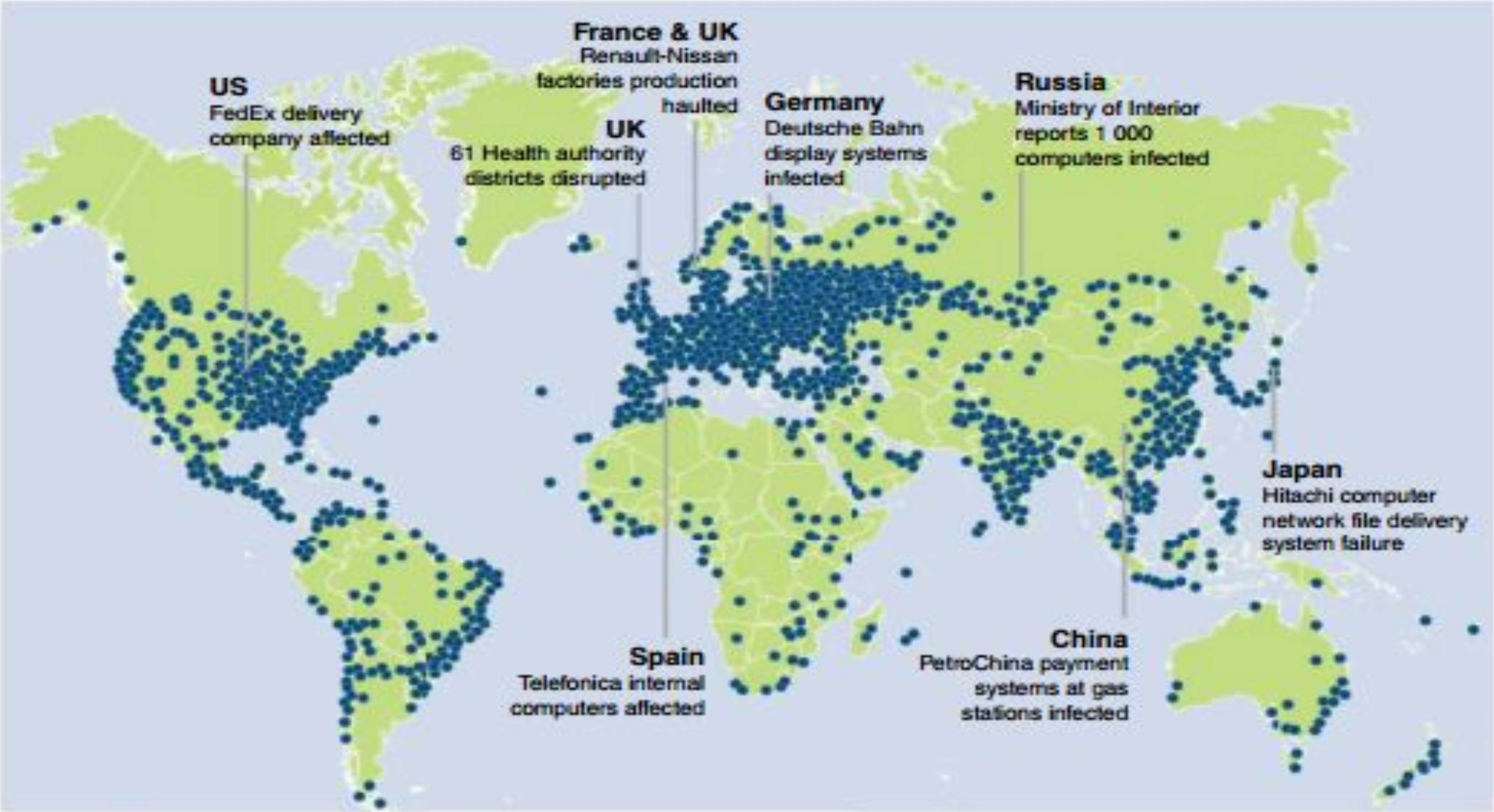

France & UK
Renault-Nissan factories production haulted
US
FedEx delivery company affected
UK
61 Health authority districts disrupted
Germany
Deutsche Bahn display systems infected
Russia
Ministry of Interior reports 1 000 computers infected
Japan
Hitachi computer network file delivery system failure
China
PetroChina payment systems at gas stations infected
Spain
Telefonica internal computers affected

FIGURE 2.2 *WannaCry* infections across the world and business impacts, May 2017.

Not Petya, 2017

- Ukrainian tax preparation program that is an industry standard for tax filing in Ukraine. As a result, 80% of the infections occurred in Russia and Ukraine, where more than 80 organizations initially reported being affected, including the National Bank of Ukraine, Kiev’s Boryspil International Airport, and the radiation monitoring system at Ukraine’s Chernobyl nuclear power plant.

- NotPetya utilized the exploit of EternalBlue, similarly to WannaCry, but enhanced it with multiple techniques to propagate throughout internal networks, including harvesting passwords and running PSExec code on other local computers.

- Maersk, one of the largest shipping operations, reported that infections of the NotPetya virus had caused it to suspend operations in parts of its organization, causing congestion in the 76 ports it operates worldwide, and resulting in business losses of up to $300 million in the initial quarter after the attack.

Antivirus Software Industry

- It contains a dictionary of templates of known malware characteristics, and compares software that it finds with these definitions. If it finds a match, it stops the code executing, quarantines it, and eradicates it safely. Typically antivirus software will also do ‘heuristic checking’ or ‘anomaly detection’ – monitoring programs for unexpected behavior that might indicate a new type of virus that isn’t in its library of known malware.
- Hackers writing malware that they don’t want to be detected have to use a new template that is not already included in the antivirus dictionaries. New forms of malware are being generated every day. And every day new forms of malware are being detected, codified, and added to the dictionary of antivirus definitions.

- The speed at which new malware can be identified and added to the antivirus dictionaries – and disseminated to all the users of the antivirus software – is a vital part of defending users.

Malware Payloads

The Types of harm the payload can cause to the host system are braodly classified into the following categories:-

1. Deletion
2. Extortion
3. Theft
4. Fraud
5. Hijacking

Risk of Malware Infection

- Bypass the protection provided by standard anti-malware security systems, how many companies the malware manages to infect, and whether your organization is among the susceptible population for the vector it uses.

- A large number of malware entry ploys exploit older and unpatched versions of common commercial software. Companies that take longer to update their software systems tend to be more susceptible to malware infection. ‘Patching latency’ – the average age and versioning of software running in an organization, relative to the latest version available – is a measure of a company’s security diligence and susceptibility to malware infection

- When Maersk was infected by the NotPetya virus, this required the reinstallation of 45,000 machines, more than 50% of the machines on the company’s internal network, taking 10 days and inflicting business losses of at least $300 million. ther organizations infected with NotPetya were luckier and had only a small number of infected machines. The lateral propagation of malware within an organization determines the likely severity of impact on the business. Lateral propagation is mainly driven by the malware programming and its ability to replicate within a network without detection and prevention by network traffic monitoring systems.

Ransomware

- Ransomware has been a common method of extorting individuals using personal computers and small businesses for some years. There are many examples of ransomware that have been developed since the first generation came into circulation around 2005, from early programs in 1989.

- Ransom demands range from $25 to $500, averaging around $300. Only a small proportion of victims pay the ransom (around 3%), but this is enough to generate significant incomes for the perpetrators.

- CryptoWall, is reported to have earned $18 million from US citizens between April 2014 and June 2015.

Cyber Extortion Attacks on Larger Organizations

- Cyber extortion has become increasingly more ambitious, targeting organizations that can afford higher payoffs or that are likely to pay for large numbers of devices to be unlocked.
  Ransomware incidents are reported more commonly in certain industries, namely healthcare, telecommunications, computer system design, and chemical and drug manufacturing sectors, while some sectors, such as manufacturing, food, and agriculture, have reported a comparably low number of incidents.

- Public-sector organizations and government departments are not immune: local administrations in Italy are reported to have paid ransoms of about €400 (US$440) to recover corrupted files. Even a US police department in Tewksbury, Massachusetts, near Boston, notoriously paid $750 in bitcoin to prevent its files from being lost. Examples include the Hollywood Presbyterian Medical Center in California, which paid a $17,000 bitcoin ransom in February 2016 for the decryption key for patient data.

- A ransomware attack that froze the payment system of the San Francisco municipal railway system, accompanied by a demand for $73,000 in November 2016, was dealt with by allowing customers to ride for free while the system was rebuilt instead of paying the ransom.15 The moral hazard of paying ransoms is that it encourages the extortionists to repeat the crime on other victims, and the money paid provides them with the resources to sustain and expand their operations.

The Business of Extortion

The extortionists have become professional at the process, including setting up call centers in third-party countries to assist the individuals that they are blackmailing with the necessary payment steps and providing technical support for the unlocking of their data, providing decryption codes for the software. Support extends to helping their victims set up bitcoin bank accounts to make untraceable payments. To avoid being traced, the call centers are quickly disbanded after a certain number of payments are extracted.

Ransomware Attacks on the Rise

- The use of ransomware, where particular malware is infiltrated into the networks of a company and disables servers or locks up data until a ransom is paid, has become more of a concern of cyber security specialists. Both WannaCry and NotPetya appeared to be ransomware when they first infected a system. This demonstrated that with the right vector and ability to exploit a susceptible population, malware can penetrate the defenses of even quite sophisticated and well protected companies.

- There are tools such as polymorphic malware generators being more commonly used, enabling large numbers of more sophisticated ransomware to be created to order. Variants of ransomware being offered for sale on the black market can demand ransom payments as high as $1 million.

- As regulatory penalties for data breaches become increasingly severe, criminals who steal data may decide that extorting the company against the threat of openly publishing the data is more profitable than selling it on the black market. Companies may be tempted to pay a ransom rather than pay severe regulatory fines.

DENIAL OF SERVICE ATTACKS

- Half of all major US companies experience a denial of service attack on their websites each year, and one in eight of those attacks overwhelms their resilience and renders their internet services unavailable.

- Traffic volumes can be generated by botnets – a network of remotely controlled zombie computers, which are personal computers infected by malicious software that sends out messages without the owner even noticing.

There are the following types of the DDos attacks

- Volumetric attacks: flood a target network with data packets that completely saturate the available network bandwidth. These attacks cause very high volumes of traffic congestion, overloading the targeted network or server and causing extensive service disruption for legitimate users trying to gain access.

- Application-based attacks, also known as ‘layer 7’ attacks, target the application layer of the operating system (open systems interconnection model). The attack does not use brute force, but is a disguised instruction that forces functions or particular features of a website into overload to disable them. It is sometimes used to distract IT personnel from other potential security breaches. Application-based attacks are reported to constitute around 20% of DDoS attacks.

- Protocol-based or Transmission Control Protocol (TCP) connection attacks involve sending numerous requests for data as synchronized (SYN) packets to the victim server – typically a firewall server – which opens a new session for each SYN packet, overwhelming the control tables of the server. These TCP SYN floods are one of the oldest types of DDoS attack, but are still used successfully.

- Fragmentation attacks use internet protocols for data re-aggregation as an attack vector to overload the processing power of a server. The fragmentation protocol manages the transmission of volumes of data by breaking the data down into smaller packets and then reassembling them at their destination. Sending confusing or conflicting protocols floods the server with incomplete data fragments.

During the DDos attacks following things occur

1. Users experience much slower page load time in their browsers.
2. Transactions fail
3. Services are unavailable

Intensity of Attack

An attack of 10 Gbps (significant intensity) is likely to overwhelm the capability of a website with the infrastructure to support around one million visitors a month, and cause it to become unavailable, if it does not have specific anti-DDoS measures in place. A website with more infrastructure and capacity is less vulnerable, and it takes more attack intensity – higher Gbps volumes – to take it down.

Duration of DDoS Attack

- The duration of attacks and the time that servers can be interrupted is a key component of potential business disruption loss. If an attack is intense enough to degrade or stop a server from functioning, the key issue for managers is the length of time that the attack can be sustained to disrupt business activities.

- The most severe DDoS attack recorded in recent years lasted for a total of three hours at 1,200 Gbps. 16 Long-duration attacks of low intensity and multiple repeat attacks are more common. The potential is evidently growing for high intensity attacks to be sustained for long durations, potentially for days at a time, but this is not yet a common characteristic of DDoS attacks.

Magnitude of DDos Attack Activity

- The number of annual DDoS attacks fluctuates significantly, but analysis of recent trends suggests that the overall number of individual attacks may not be increasing substantially. However, attacks are getting more intense, with a greater proportion of attacks being of higher intensity and sustained for longer durations.

- However, the large majority of attacks are destructive, with only indirect or no monetary benefit to the perpetrator. Some DDoS attacks mask other criminal activities, such as a simultaneous breach of a network to steal data. Some may even be accidental or collateral damage from attacks.

The Big Cannons

- External agents, or as a method of augmenting military actions in a conflict. A number of countries are known to have military or state-sponsored units with powerful DDoS capability, such as the Chinese ‘Great Cannon’ and the US National Security Agency QUANTUM internet attack tool.

- Over a half of all recent attacks are multi vectored, making them more difficult to mitigate. Attacks most commonly originate from, or are routed through, servers in China, although attacks are directed via servers in many countries, including the United States, Turkey, Brazil, South Korea, and other territories.

- An HP Fortify study found that as many as 70% of IoT devices are vulnerable to attacks due to weak passwords, insecure web interfaces, and poor authorizations, and new vulnerabilities are being discovered each year.

- There have been high-profile cyber attacks that have succeeded in penetrating the volume wholesale financial transaction systems operated by financial institutions. Sophisticated threat actors have penetrated the SWIFT banking system, the Polish financial regulator, and individual bank-to-bank trading systems.

- The attacks compromised more than 100 financial institutions, with loss estimates as high as $1 billion. The criminals exploited vulnerabilities in Microsoft Office via spear phishing emails (targeted fraudulent emails) to gain access to money processing services, ATMs, financial accounts, and the SWIFT network, giving the cyber criminals a means to move and transfer money.

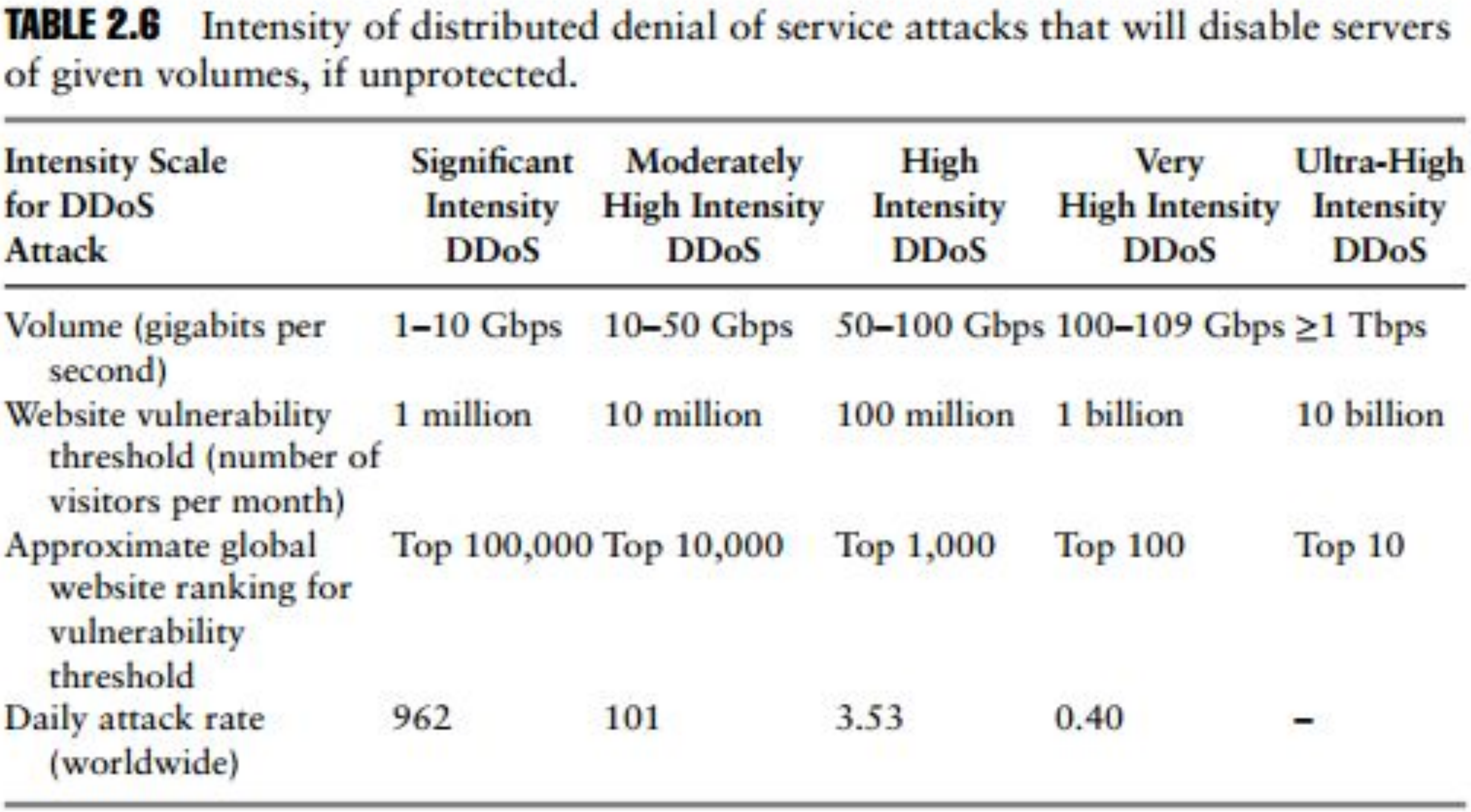


TABLE 2.6 Intensity of distributed denial of service attacks that will disable servers of given volumes, if unprotected.

Intensity Scale for DDoS Attack	Significant Intensity DDoS	Moderately High Intensity DDoS	High Intensity DDoS	Very High Intensity DDoS	Ultra-High Intensity DDoS
Volume (gigabits per second)	1–10 Gbps	10–50 Gbps	50–100 Gbps	100–109 Gbps	≥1 Tbps
Website vulnerability threshold (number of visitors per month)	1 million	10 million	100 million	1 billion	10 billion
Approximate global website ranking for vulnerability threshold	Top 100,000	Top 10,000	Top 1,000	Top 100	Top 10
Daily attack rate (worldwide)	962	101	3.53	0.40	–

Risk in the IT Supply Chain

- Modern system design increasingly integrates software components and outsourced or third-party services into offerings.There are many potential counterparties of an organization that could cause the organization a loss. Any counterparty that has access to the company's data, particularly those that may be using, generating, or processing the type of data.
- Third-party software products provide their own vulnerabilities and present a risk of triggering a loss to an organization if failures occur. There are many examples of failures in commercial and third-party software that have caused large-scale losses. Examples include flaws in scanning algorithms that randomly alter numbers in the digitization capture of printed documents,34 banks having to write down large losses resulting from errors in software calculations of interest rates,35 and errors in software parameters of industrial control systems resulting in substandard product manufacturing and major product recall.

- The trend towards systems integration from multiple third-party components make these issues of dependency and supply chain risk even more acute. As businesses pull data streams from other people’s application programming interfaces (APIs) and apply multiple algorithms from different providers, even diagnosing malfunctions will become highly complex: when two different artificial intelligence algorithms combine and produce unexpected outcomes, whose responsibility is it?

The Risk of CSP Failures

Cloud computing has seen very rapid uptake to become a major driver of the digital economy, with expenditures on public cloud computing having doubled every four years and now being used in some capacity by more than 90% of companies 37 to generate up to $246 billion in revenue worldwide.

Most adoption is currently piecemeal, with many managers concerned about governance of the use of CSPs internally, combating this ‘shadow IT culture’, and developing an integrated strategy for cloud adoption. Many organizations may be more exposed to cloud outages than they realize. Experienced managers advocate a structured approach to cloud adoption that follows six stages of putting business activities onto the cloud:

1. Data storage (low value)
2. Delivery of scalable SaaS (non-revenue)
3. Data storage (higher value)
4. Migration of existing apps
5. Building (new) revenue streams
6. Tackling legacy systems and replacing them with cloud equivalents

Industry analysts grade the levels of cloud adoption of organizations into five levels:

1. No plans
2. Cloud watchers (planning for cloud activities)
3. Cloud beginners (carrying out their first cloud projects)
4. Cloud explorers (having apps running in the cloud)
5. Cloud focused (making heavy use of multiple apps)

Surveys suggest that around a third of companies currently may be ‘cloud focused’ and making heavy use of the cloud. This proportion is higher in small and medium-size businesses (38%) than large enterprises (28%).
There are a number of ways that CSPs could suffer an outage that affects their customers. These include:

- Mechanical failure of equipment, fires, or physical damage of server sites
- Power failure or other essential utility provision, including failure of the backup generators or cooling systems
- Cyber attack by malicious external actors seeking to disrupt services or steal data
- Internal software system failure by accident or from a malicious insider

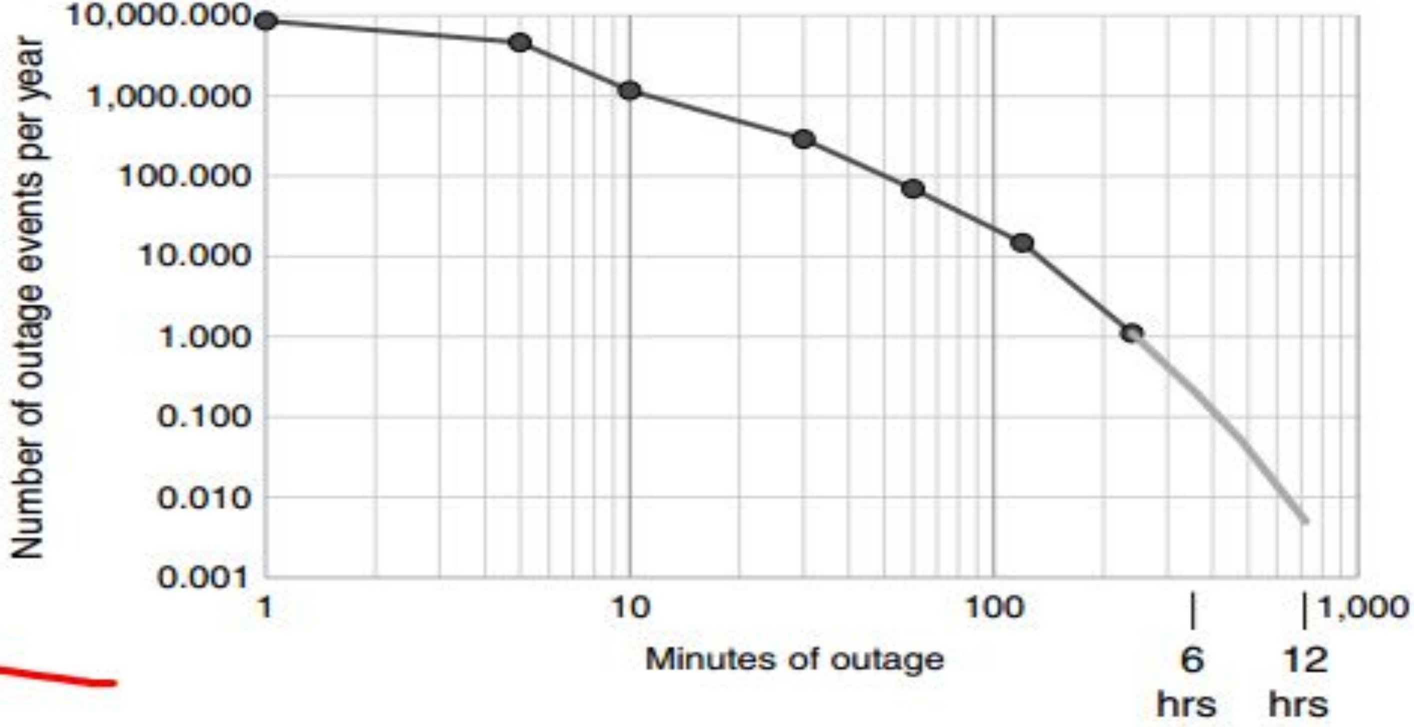


FIGURE 2.7 Duration of cloud service outages reported in a single year (2017 statistics for 100,000 events) extrapolated for likelihood of longer outage events per year.

Nevertheless, system failures do occur and customers suffer outages. On February 28, 2017 Amazon’s Simple Storage Service (S3) saw ‘high error rates’ in multiple AWS services in the US eastern region, which escalated to cause a four-hour outage, and quickly cascaded to other regions and services, including CloudWatch, EC2, Storage Gateway, and AWS Web Application Firewall (WAF). The outage was triggered by an AWS S3 team user error, providing incorrect commands while debugging. This outage affected the websites of around 148,000 AWS customers – initially losing graphics and slowing up performance, but cascading to other services and causing complete website failure.

Hypervisors are also susceptible to other attack vectors such as through network services and denial of service attacks.

It is rare that a failure causes the entire cloud service to suffer an outage. More typically a failure occurs in a single service or a single geographical region. Because of the interconnected architecture of the CSP services, if the failure cascades, it can affect other applications and spread to other geographical regions.
A typical hierarchy of outages is:

- Individual application failures for users of a particular cloud service in a specific region
- Failure of a specific application across multiple regions
- General service failure (multiple applications) for all customers of a particular region
- General service failure (multiple applications) for all customers of multiple regions