



Risk Type Overviews

Publication Date – April 19, 2023

What Are the BitSight Risk Types?

Risk Categories

There are four primary risk categories: Compromised Systems, Diligence, User Behavior, and Public Disclosures.

Compromised Systems

The Compromised Systems risk category accounts for 27% of a company's BitSight Security Rating.

This risk category indicates the presence of malware or unwanted software, which is evidence of security controls failing to prevent malicious or unwanted software from running within an organization.

A compromised system can lead to a disruption in daily business operations and can increase the risk of data breach.

Separate instances of malware communications, even if it is from the same machine, constitutes a single observation.

Compromised Systems Risk Vectors

We collect information about a wide range of security events. These events are categorized among the following risk vectors:

- [Botnet Infections](#)
- [Spam Propagation](#)
- [Malware Servers](#)
- [Unsolicited Communications](#)
- [Potentially Exploited](#)

Service Providers

Service provider companies might be hosting some of their customer's infrastructure on their networks. As a result, some Compromised Systems events observed on service provider networks can be due to their customer's activity.

- Service providers are identified with a "Service Provider" label in their company overview page.
- Compromised Systems findings that belong to an organization's service provider(s) are marked with a (†) Dagger icon.

Remediation

At a high level, IP addresses can be used to locate the source of infections. If an organization has a small number of IP addresses, the timestamp activity can be cross-checked with router logs.

For larger organizations or those behind several layers of network routing, the [Forensics](#) package provides additional levels of information about Compromised Systems that response teams can use to better pinpoint sources of infections and compromise, such as source ports and destination ports. The Forensics add-on also provides a powerful set of record filters for finding compromised systems.

- Conduct a thorough security review of the machine (malware & antivirus sweep).

- Review services used on the machine and harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

Diligence

Diligence accounts for 70.5% of a company's BitSight Security Rating.

This risk category assesses the steps a company has taken to prevent attacks, their best practice implementation, and risk mitigation (e.g., server configurations) to determine if the security practices of an organization are on par with industry-wide best practices.

Diligence Risk Vectors

Diligence findings are categorized among the following risk vectors:

- [SPF Domains](#)
- [DKIM Records](#)
- [TLS/SSL Certificates](#)
- [TLS/SSL Configurations](#)
- [Open Ports](#)
- [Web Application Headers](#)
- [Patching Cadence](#)
- [Insecure Systems](#)
- [Server Software](#)
- [Desktop Software](#)
- [Mobile Software](#)
- [DNSSEC Records](#)
- [Mobile Application Security](#)
- [Domain Squatting](#)

Remediation

Search for Diligence findings from the Findings page.

Advisory remediation tips instructing how to resolve the issue are available to help improve the grade as it no longer negatively affects the overall risk vector grade. Some remediation tips are more detailed than others, depending on the complexity or prevalence of the issue.

WARN and BAD findings have remediation text as part of the finding details pop-up, along with the issues in question. If there are additional ways to improve on the findings that are in line with current industry best practices, remediation text is also available for some GOOD, FAIR, and NEUTRAL findings.

User Behavior

The User Behavior risk category assesses employee activity, such as file sharing and password re-use. These types of activities can introduce malware to an organization or result in a data breach. It accounts for 2.5% of a company's BitSight Security Rating.

User Behavior records that are older than 60 days no longer affect a company's grade. User Behavior records are updated daily.

User Behavior Risk Vectors

- [File Sharing](#)
- [Exposed Credentials](#)

Public Disclosures Risk Category

The Public Disclosures risk category provides information related to possible incidents of undesirable access to a company's data, including breaches, general security incidents, and other disclosures. Information is collected from verifiable news sources, both domestic and international, and by filing Freedom of Information Act (FOIA) requests.

Though these events do not necessarily result in data loss, the interruptions to business continuity are relevant and can be used to improve security preparedness.

Public Discovery

The earliest date when information pertaining to the security incident became publicly available either via news sources or filing with regulatory bodies, when an incident was self-discovered & the date of discovery publicly available, or the date when affected parties were notified. When major headline news of unauthorized access is disclosed, we add it to our system within the same week. Note that having knowledge of the actual date of the incident is rare, even to the affected company.

Effective Date

The date when a Security Incident event was recorded in the BitSight platform.

Public Disclosure Risk Vectors

- [Security Incidents](#)
- [Other Disclosures](#)

Botnet Infections Risk Vector

This risk vector indicates that devices on a company's network are participating in a botnet (combination of "robot" and "network"), either as bots or as a command and control (C&C or C2) server.

Malware Classification

When classifying observations as Botnet Infections events, we use criteria similar to antivirus vendors to differentiate malware from potentially exploited systems. The criteria includes the capability and intent to install additional programs on the system without user consent.

Depending on the number of affected companies, we may:

- Perform an in-depth study.
- Document the malware family in an internal document or in our blog. This may include a short description of the malware and its capabilities.
- Use a list of samples and sandbox execution IOCs as evidence of maliciousness. These can be independently validated by any interested party.

Examples

- **Kelihos:** Used for Bitcoin theft and to send spam.
- **Torpig:** Designed to steal sensitive user data, such as usernames, passwords, login locations, and personal and corporate credit card information. It is typically spread by the Mebroot rootkit.
- **Zeus:** Steals specific types of data, such as banking information and other login credentials. It can also be used to install other malware, such as CryptoLocker ransomware.

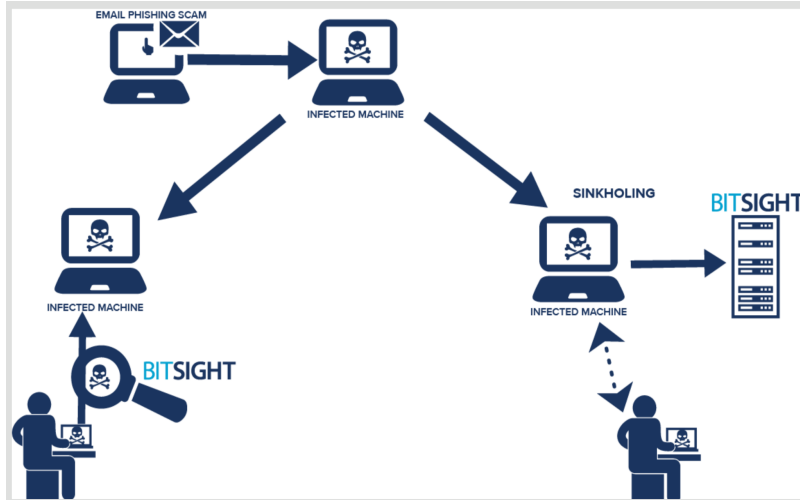
Data Collection Methods

Botnet Infection events are identified through evidence that one or more devices in a company's network are observed to be participating in a botnet.

Botnet activity is observed using honeypots and sinkholing technology. We have multiple methods of detecting and intercepting traffic from a botnet and attributing it to a specific company's network.

- The IP information from the data sources are matched with those of a company.
- For botnets using domain generation algorithms, we register a set of randomly generated domains and wait for devices to connect to them.

The following illustration demonstrates our infection detection method:



- By monitoring known botnets and attributing the IP address of the connecting infected device back to a company (left).
- By intercepting communications between an infected device and a command and control server (C&C or C2 server), through sinkholing (right).

Risks

Botnets can be used to exfiltrate sensitive data (such as corporate secrets and user information), repurpose company resources for malicious activities (such as distributed denial-of-service attacks or cryptocurrency mining), and they can serve as conduits for other infections.

Companies with a Botnet Infections grade of B or lower are more than twice as likely to experience a publicly disclosed data breach.

Botnets can deliver high-volume network attacks and perform large-scale tasks, such as:

- Generate Bitcoin and other cryptocurrencies, which is abuse of local machine resources (increased CPU/RAM/HDD usage) and takes away cycles from legitimate users.
- Distribute spam or malware, which can potentially steal data and put an organization's confidential information and infrastructure at risk.
- Network attacks from company servers to their targets, such as DDoS. Company reputation can be damaged; servers blacklisted; company could unwittingly participate in DDoS or other large-scale network attacks against itself.

Remediation

- Conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

Findings

Finding Details

Field	Description	Sorting & Filtering
Finding Identifier	The IP address of the finding.	Sort
First Seen	The date of the first observation.	<ul style="list-style-type: none">• 7 Days• 1 Month• 3 Months• Custom
Last Seen	The date of the most recent observation.	<ul style="list-style-type: none">• 7 Days• 1 Month• 3 Months• Custom
Grade	The record grade of a Diligence risk vector (GOOD, FAIR, NEUTRAL, WARN, or BAD).	N/A
Details	Details of this finding.	No
Infection	The name of the botnet.	No
Duration	The duration of the botnet has been observed.	No
Details	A description of the botnet.	No
Targeted Platform	The types of affected machines.	No
Risks	A summary of risks.	No
Remediation Instructions	Resources for remediation.	No
Assets	The number of affected assets (IP or domain) and its importance.	No
IP Attributions	The reason why the IP was attributed to the company.	No
Comments	Discussions around the event.	No

Forensic Details

Available with the Event Forensics add-on package:

Field	Description
GeoIP Location	Example: US
Source Port	The source port number.
Destination Port	The destination port number.
C&C IP	The IP address of the command and control server.
Observation Count	The number of observations.
Detection Mechanism	The mechanism used to detect botnet activity. Example: p2p
Representative Event Timestamp	The date and time of the finding.

Spam Propagation Risk Vector

This risk vector is composed of spambots, where a device on a company's network is unsolicitedly sending commercial or bulk email (spam). If spam originates from email addresses or devices within a company's network, this is an indication of an infection.

If a company offers a bulk email-sending service, such as a digital marketing company that sends marketing material on behalf of their customers, they are excluded from this risk vector. These companies are identified with a "Bulk Email Sender" label on their company overview page.

Bulk Email Sender

Malware Classification

When classifying observations as Spam Propagation events, spambots are identified based on known patterns contained in the email headers that are common across malware families, such as the subject field, the "Received From" field, email addresses, and various IDs.

Examples

One type of observed spam mechanisms are spambots. Spambots are used for simultaneously sending bulk email messages from multiple devices.

Data Collection Methods

Spam Propagation events are when malware sends unsolicited email (spam), known as "spambots." If spam originates from email addresses or devices within a company's network, this is an indicator of an infection.

Spam activity is observed using:

- Email Header Analysis
- Honeypots
- Mail Server Connection Analysis
- Sinkholes
- Spam Traps

If resources are limited, you do not have a packet analyzer, are on a time constraint, or are not seeing a large volume of events, doing nothing may be the correct risk management decision for your business. BitSight Security Ratings are intended to help prioritize your cybersecurity risk management activities. If limiting spam propagation is low priority, then the rating can be used to make this decision more data-driven.

General Indicators

The following examples are clear indications of spambot activity:

- **Port 25:** Search for port 25 activity from machines in your company firewall logs.
- **Known Spambots:** Include "spambot" as a keyword and the following spambots in your search:
 - Asprox

- Cutwail
- Necurs
- Lethic
- Impossible HELO
- Most machines are generally behind a router. If spambot activity is coming from computers behind a router:
 - **Firewall:** Check your firewall logs to correlate timestamps of spambot event details with outgoing mail events.
 - **Forensic Details** Use the destination port as another indicator to find your internal IP address associated with spambot activity.
 - **Timestamp:** If spambot activity is coming from computers behind a router where your mail server is also located, use timestamp records to correlate outgoing mail activity.

“Impossible HELO” Records

These events can be difficult to locate, since they did not result in a sent message.

- If you are running a packet analyzer, search for the reported “helo [impossible domain]” in your logs.
- Ensure your understanding of [HELO announcements](#) from your mail server are aligned with [RFC-2821](#).
- Check your [HELO configuration](#) for possible errors.

Additional Indicators

If you are still unsuccessful:

- **Malware Detection:** Check your systems for malware. Run malware detection on your systems that may be sending traffic through the IP address.
- **Email Permissions:** Check if any machine on this network is permitted to send email. If you have a packet analyzer (such as [Snort](#), [Suricata](#), or NetFlow) turned on for port 25 connections behind a Network Address Translation (NAT):
 - **With no mail servers:**
 - Block all port 25 connections. If port 25 is allowed connections again, the undiagnosed infected machines on your network are still present and could engage in malicious activity. If the malware also makes communications via port 80 or 443, it may be captured via a sinkhole and reported as a Botnet Infection or Potentially Exploited event, but this correlation is not guaranteed.
 - Block port 25 on your network. Only allow outgoing connections to mail services your organization is known to, or is planning to, use for internal/external email communication.
 - Leave port 25 open, install a packet analyzer, and watch for announcements or messages from machines that are not designated mail servers or which match header information reported on your rating.
- **With mail servers:** Watch which header information matches the reported headers.
- **Analyzer Search:** Search the records for “helo [impossible domain].” If headers are preserved in these logs, look for records that are not mail servers and have port 25 as the destination port.

Risks

- Damage to a company’s reputation.
- Abuses company resources.

- Legitimate email from the company may be flagged as spam and will not reach its intended recipient.
- Increases the risk of additional malware entering organizational systems.

Remediation

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

Findings

Finding Details

- **Spam Type:** The type of spam.
- **Detection Method:** The method used to detect the observation.

Event Forensics

To protect BitSight data sources, destination mail server information or destination IP addresses are not provided. Use the source IP address and IP block ranges in your infrastructure as a compass to narrow your search for spambots. Spambot activity in the source IP address may not be the same IP address of your company mail servers.

When searching for events and records, the resulting list may represent a subset of the full listing that's limited by count (up to 2,500). This is due to large companies that can have outstanding volumes of events that may become impractical to manage. The listing must be reasonably sampled to a size that can still be supported. All risk vectors that should affect the rating are included in the sample.

Includes Compromised Systems fields (Location, Sender IP Address, Date Seen, First Seen, Last Seen, Representative Timestamp) and the following fields:

Field	Description
Sender Address	The sender of the spam email.
Email Subject	The subject line of the spam email.
Observations	The number of times the spam propagation was observed in a 24-hour period, between midnight UTC one day and midnight UTC the next day.
Spam Type	The method or tool used to send bulk spam email - Snowshoe, Darkmailer, etc.
Detection Mechanism	<p>This method was used to detect the infection.</p> <p>Example: A botnet infection could be detected using a sinkhole that tricked a bot into connecting to it, instead of the command and control server. Spam propagation could also be discovered by analyzing email headers.</p>



Availability for these fields vary based on the detection method.

Malware Servers Risk Vector

This risk vector is an indication that a system is engaging in malicious activity, such as phishing, fraud, or scams. A company's network is hosting malware that is meant to lure visitors to a website or send a file that injects malicious code or viruses.

Risks

Compromised servers can put other devices at risk of infection, simply by connecting to the company's resources, which can result in a disruption in business continuity, exposure to additional malware threats, and an increased risk of data breach or data loss.

- **Data Exfiltration:** Malware can observe and report behavioral information, corporate secrets, or personally identifiable information (social security number, home address, telephone number, email address, etc.).
- **Unauthorized access:** The malware is able to obtain administrative (super-user) access on the machine by stealing usernames and passwords and can disable security or antivirus software.
- **Implies other infections:** The malware is often a staging ground for additional malware or viruses to compromise the system. Malware that allows other software to get in (such as adware, spyware, botnets) is called a "backdoor." Viruses subject the targeted organization to risk of data loss and reputation damage.
- **Resource abuse:** The malware uses up disk space, delete files, erase hard drives, network bandwidth, computer memory (increased CPU/RAM/HDD usage) for malicious purposes to perform behind-the-scenes internet fraud. Takes away cycles from legitimate users.

Remediation

One strategy for protecting against malware is to prevent the malware software from gaining access to the target computer.

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

Unsolicited Communications Risk Vector

This risk vector indicates a host is trying to contact a service on another host. It might be attempting to communicate with a server that is not providing or advertising any useful services, the attempt may be unexpected, or the service is unsupported. This also accounts for hosts that might be scanning darknets.

Risks

This type of activity not only shows that a device is compromised, but that it is actively seeking other devices to infect and also risks opening a back door for malware to infiltrate systems.

Remediation

One strategy for protecting against malware is to prevent the malware software from gaining access to the target computer.

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

Potentially Exploited Risk Vector

This risk vector indicates that a device on a company's network is running a potentially unwanted program (PUP) or potentially unwanted application (PUA).

Risks

The presence of these applications suggests users within the corporate network are able to install unvetted applications or programs and can allow more harmful malware to compromise the system.

Potentially unwanted applications can create risk for organizations, as they may cause users to visit malicious sites, gather information while a computer is in use (including browsing history, search queries, account credentials, etc.), or allow attackers to take control of the compromised machine.

Remediation

One strategy for protecting against malware is to prevent the malware software from gaining access to the target computer.

- Track down infections and conduct a thorough security review of the machine (malware & antivirus sweep).
- Review services used on the machine, harden firewall rules.
- Improve employee computer safety training (phishing, installing unapproved software).

SPF Domains Risk Vector

This risk vector assesses the effectiveness of Sender Policy Framework (SPF) records, which are DNS records that identify mail servers permitted to send email on behalf of a domain. Properly configured SPF records ensure that only authorized hosts can send email on behalf of a company by providing receiving mail servers the information they need to reject mail sent by unauthorized hosts.

Only domains that are sending email and have not implemented SPF are assessed for this risk type.

Risks

Without SPF records, attackers can pose as legitimate senders from trusted domains. This makes it difficult to trace a message to its source and easy for spammers to hide their identity.

Remediation

- Create an SPF record.
- Check for common mistakes in your SPF record. An effective SPF record has the following characteristics:
 - Has one “all statement” or a “redirect,” but not both.
 - The all statement appears at the end of the record.
 - Does not give neutral or pass to the all statement. Any redirect occurs after all other mechanisms.
 - A company's total SPF grade is based on the assessment of the top level record as well as the records of the domains specified in the includes and redirects up to two levels below.
 - Macro expressions are checked to verify they are formed properly, where applicable.
- All domains should have SPF records, even SMTP servers and those that aren't configured to send mail. If a company does not intend to send mail from a domain, an attacker can still use that domain to spoof email.

DKIM Records Risk Vector

This risk vector assesses the effectiveness of DomainKeys Identified Mail (DKIM) records, which is a countermeasure against adversaries that are attempting to send fake email by using a company's email domain. Properly configured DKIM records can ensure that only authorized hosts can send email on behalf of a company.

The protocol allows receiving email servers to check if the sending domain is authorized. An encrypted signature is placed inside a DKIM-protected email. It's checked by a recipient against the sender's public DKIM record (another key). The signature in the email is then decrypted by the recipient using the key to confirm the sender's authenticity.

Risks

Without DKIM records, a company may not be effectively preventing email from being spoofed from its domains. This makes phishing attacks easier and makes the organization susceptible to any number of intrusions that can put the organization's information, employees, and customers at risk.

Remediation

We follow NIST recommendations:

- Search for Diligence records and then implement an effective DKIM record if one does not already exist. See our comprehensive article on [How to create a DKIM record](#).
- Generate a new [RSA keypair](#), specifying a bit strength of 2048 or larger. For elliptic curve keys, a length of 224 bits is recommended. Refer to the [recommended key length](#). We follow NIST recommendations regarding key length.
- Refer to the [recommended key rotation](#) for how often to generate a new RSA keypair.
- Check that your keys are properly stored and the DKIM record has the correct key.

References

- [NIST: Special Publication 800-177](#)
- [NIST: 800-131A \(See Section 3\)](#)
- [DKIM RFC \(RFC-4871\)](#)
- [Wikipedia: DomainKeys Identified Mail](#)
- [Google: Internet-wide efforts to fight email phishing are working](#)
- [Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths](#)

TLS/SSL Certificates Risk Vector

This risk vector evaluates the strength and effectiveness of the cryptographic keys within [TLS and SSL certificates](#), which are used to encrypt internet traffic. Certificates are responsible for verifying the authenticity of company servers to associates, clients, and guests, and also serves as the basis for establishing cryptographic trust.

Risks

When communications are not properly secured or encrypted, traffic sent to the host are unencrypted. Personal customer or employee information, including passwords, can become publicly visible to observers and may lead to data breaches.

Remediation

- Review the [Certificate Authority Best Practices](#) and implement effective TLS/SSL certificates.
- Obtain valid and up-to-date TLS certificates from an [industry certificate authority](#).
- Select a stronger signature algorithm (like SHA-256).

TLS/SSL Configurations Risk Vector

This risk vector determines if the used security protocol libraries support strong encryption standards when making connections to other machines. TLS/SSL is a widely used method of securing communications over the Internet.

Risks

- Incorrect or weak TLS/SSL configurations can make servers vulnerable to certain attacks, including POODLE and Heartbleed, and can allow attackers to have access to sensitive information.
- SSL and early TLS (TLS 1.0 and TLS 1.1) no longer meet the security needs of organizations, with regards to implementing strong cryptography to protect payment data over public or untrusted communications channels.

Remediation

- Update and keep server implementations of TLS/SSL (OpenSSL, LibreSSL, etc); latest versions are patched against known vulnerabilities and they have countermeasures for other attacks.
- Refer to the TLS 1.0 and 1.1 deprecation schedule to see how this risk vector will be affected. Disable SSL v2, SSL v3, TLS 1.0, and TLS 1.1. Migrate to a minimum of TLS 1.2. Migrating to a later version (TLS 1.2 or TLS 1.3) is strongly encouraged.
- Regenerate Diffie-Hellman primes to be 2048 bits.
- Refer to the [Guide to Deploying Diffie-Hellman for TLS](#) to configure TLS securely.
 - Ensure secure TLS cipher suites and key sizes are supported and use key exchange methods that support perfect forward secrecy.
 - Disable support for other cipher suites that are not necessary for interoperability.

Open Ports Risk Vector

This risk vector observes ports that are exposed to the Internet, known as “open ports.” While certain ports must be open to support normal business functions and few companies will actually have no ports open, the fewer ports that are exposed to the Internet, the fewer openings there are for attack.

Risks

A potential attacker can externally scan for open ports to determine which software or services to target. Open ports with outdated protocols or with protocol vulnerabilities provide potential entry points for attackers to access a company’s network.

Remediation

This is the most heavily weighted risk vector in the Diligence risk category. This should be the focus of a company’s remediation and process improvement efforts.

- Embedded in every packet of network communication is the port number for that communication, which can be used to identify and block unwanted attempts to communicate over certain ports or ranges of ports not used by the company.
- Audit the services running on a particular machine and ensure only vital services are running.
- Set up access to required services over a Virtual Private Network (VPN).
- Block specific or ranges of ports not used by the company in the company edge network infrastructure. The port number is embedded in every packet of network communication, which can be used for port identification. View the full list of network ports in the [IANA Service Name and Transport Protocol Port Number Registry](#).

Rating Details

The Open Ports risk vector assessment is based on the number of findings an organization has and the security measures in place around those open ports.

There are different grades for when there is typical service and detected service port activity.

- We assess detected services.
- If no service is detected on the port, we assess typical services.
- Some ports are potentially vulnerable, where the level of risk varies. Potentially vulnerable open ports do not have a set impact on the Open Ports letter grade.

When a port is found to be fixed to a certain network protocol or software (such as port 143 for IMAP services), it’s attributed to typical service activity on that port unless the cause can be determined as something else. If a service is detected, this will override the typical service running on that port for grading purposes.

While very few companies will actually have no ports open, the fewer ports that are exposed to the Internet, the fewer opportunities there are for attack.


Impact

Only Open Ports records that were observed in the last 60 days are factored into the Open Ports letter grade. Since the infrastructure of a company is continuously updated, records are set to expire if no Open Ports records were observed within the past 60 days.

- If a record is verified to be opened and closed on the same day, it continues to impact the grade into the following day.

Example: A record is observed on January 1 at 8:00, and then closed shortly after at 11:00. The record's impact on the grade is removed on January 2, rather than removed on the same day of the observation.

- If the referenced IP of an Open Ports record has an “end date,” it can no longer be refreshed and will no longer impact the grade when it completes its lifetime.

Field	Description	Value
Lifetime	The letter grade will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	60 Days
Letter Grade in the Absence of Records	Companies are not required to run open port services. The rating is positively impacted if there are no records for this risk vector.	 - “A” Letter Grade
Scan Frequency	A check for observations is initiated, e.g., newly observed Diligence records or an existing record was remediated.	30-60 Days
Refresh Processing	The processing time for a manually initiated scan.	2-3 Business Days
Grace Period	The time before a recognized record starts to impact ratings.	<ul style="list-style-type: none"> • New records immediately impact the grade. • Updated records impact the grade upon the detection of a closed port. <ul style="list-style-type: none"> ○ Closed TCP ports are immediately detected and marked as “closed” within 10 days. ○ Closed UDP ports are undetectable and marked as “closed” after the record completes its lifetime (60 days).
Weight	Out of 35% in Diligence.	13%

Evaluation

The Open Ports risk vector letter grade is determined by assessing the number of specific records that are evaluated as GOOD, FAIR, NEUTRAL, WARN, or BAD:

- If the service is secure and used for normal business functions, such as SSH, the port is classified as “GOOD.”

Example: Port 23 is typically used for Telnet. It’s graded as “BAD.” However, if SSH running on port 23 is detected instead, that record would be marked as “GOOD.”

- If the service is used for normal business functions, but does not use encryption or other security measures, such as HTTP, the port is classified as “NEUTRAL.”
- Services that are rarely necessary for business functions or that have known vulnerabilities are classified as “WARN” or “BAD,” depending on the security risk of leaving them open.

Web Application Headers Risk Vector

The Web Application Headers risk vector, formerly known as “Application Security,” analyzes security-related fields in the header section of communications between users and an application. They contain information about the messages, determine how to receive messages, and how recipients should respond to a message.

Much like a business letterhead, headers explain where the message is going and who it’s from, date sent, what type of message it is, and other configuration options. They’re included in all back-and-forth communications between applications. Web servers and web-connected applications must conform to a certain set of language (communication) standards when sending information over the Internet. These language definitions are called “protocols.”

Web Application Headers cover security risks posed to an organization's application users through Hypertext Transfer Protocols (HTTP) headers. HTTP defines the way a website should respond when it can't find something, if it can find something, or something was temporarily moved. For example, the “404” page (page not found error) can be understood by your web browser thanks to the HTTP standard. Otherwise, web programmers might pick obscure numbers or other ways to tell you that a page is not found. Your browser will then have to guess.

Required headers are important for preventing communication attacks, between applications, from succeeding. Using proper Web Application Headers over the Internet ensure communications are robust against attacks that are designed to take advantage of ambiguity (communication details that are not explicitly defined).

Since Web Application Header findings are based on the entire header configuration and not on individual errors, record grades can't be pre-assigned without evaluating the entire record.

A variety of HTTP headers are assessed to determine if security best practices are being followed. Only the HTTP headers of hosts that return HTTP 200 responses are assessed. See the list of responses and how they're assessed.


Records that indicate the presence of any HTTP links or references embedded in an HTTPS website will be graded as “BAD.”

Learn more about why HTTPS is preferred over HTTP:

- [National Cyber Security Centre: Serve websites over HTTPS \(always\)](#)
- [Troy Hunt: Here's Why Your Static Website Needs HTTPS](#)

Impact

Field	Description	Values
Lifetime	The letter grade will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	60 Days

Letter Grade in the Absence of Records	<p>This is set in the center of the grading scale for computing into security ratings.</p> <p>Some records cannot be traced back to specific companies due to the use of third party systems; such as web filters and Content Delivery Networks (CDN), that are capable of redirecting and encapsulating network traffic. Some firewalls might also be detecting and blocking external scanning tools from getting any data.</p>	 - "C" Letter Grade
Scan Frequency	A check for observations is initiated, e.g., newly observed Diligence records or an existing record was remediated.	60 Days
Refresh Processing	The processing time for a manually initiated scan.	3 Business Days
Grace Period	The time before a recognized record starts to impact ratings.	<ul style="list-style-type: none"> • New records immediately impact the grade. • Remediated records: <ul style="list-style-type: none"> ○ The newest record replaces the past record and impacts the grade for 60 days, as it completes its lifetime. ○ The previous record is replaced and stops impacting the grade.
Weight	Out of 35% in Diligence.	3%

Relative Weight of Web Application Header Findings

Type	Weight
HTTPS to HTTP Redirect	Heavy
WWW-Authenticate (Error #401)	Medium
Mixed HTTP & HTTPS Content	Medium
HTTP Header	Light

Content Checks

- Websites with mixed HTTP and HTTPS content.
- Intra-site URLs are evaluated for HTTPS protocol use.
- Redirects from HTTPS to HTTP.
- Check if the “WWW-Authenticate” is contained in an HTTP 401 response from non-HTTPS events.

Assessed Headers

- Access-Control-Allow-Origin
- Cache-Control
- Content-Security-Policy
- Expires
- HTTP Strict-Transport-Security
- Set-Cookie
- X-Content-Type-Options
- X-Frame-Options (Frame-Options)
- X-XSS-Protection

Required Headers

These are important for preventing attacks and are checked for usage and correct configurations. If an application header record exists and the required header is not found in the records, the company is penalized on missing headers. The penalties are described below under “Configuration Requirements.”

Header	Required For
Cache-Control	HTTP/1.1
Content-Security-Policy	<ul style="list-style-type: none">• HTTP/1.1• HTTP/1.0
Expires	HTTP/1.0
HTTP Strict-Transport-Security (HSTS)	<ul style="list-style-type: none">• HTTP/1.1• HTTP/1.0
X-Content-Type-Options	<ul style="list-style-type: none">• HTTP/1.1• HTTP/1.0
X-Frame-Options	HTTP/1.0

Optional Headers

Optional headers may be present, in addition to required headers.

- If present, optional headers are verified that they are configured correctly and go towards the requirements as a whole for a **GOOD** or **FAIR** record grade.
- If not present, companies are not penalized since they are unnecessary for preventing malicious actions.

Header	Optional For
Access-Control-Allow-Origin	<ul style="list-style-type: none">• HTTP/1.0• HTTP/1.1
Location	<ul style="list-style-type: none">• HTTP/1.0• HTTP/1.1
Set-Cookie	<ul style="list-style-type: none">• HTTP/1.0• HTTP/1.1
WWW-Authenticate	<ul style="list-style-type: none">• HTTP/1.0• HTTP/1.1
X-XSS-Protection	<ul style="list-style-type: none">• HTTP/1.0• HTTP/1.1

Configuration Requirements

Requirements for **GOOD** grade: No more than 25% distinct misconfigured headers can be present (required and optional)

Requirements for **FAIR** grade: No more than 50% distinct misconfigured headers can be present (required and optional)



For HTTP connections, no headers are graded unless `Set-Cookie` is defined. The record grade will default to **NEUTRAL**.

Required HTTP 1.1 (HTTPS):

- Content-Security-Policy
- HTTP Strict-Transport-Security
- X-Content-Type-Options
- Cache-Control

Required HTTP 1.1 (non-HTTPS):

- Content-Security-Policy
- X-Content-Type-Options
- Cache-Control
- Set-Cookie

Required HTTP 1.0 (HTTPS):

- Content-Security-Policy

- HTTP Strict-Transport-Security
- X-Content-Type-Options
- Expires
- X-Frame-Options

Required HTTP 1.0 (non-HTTPS):

- Content-Security-Policy
- X-Content-Type-Options
- Expires
- X-Frame-Options
- Set-Cookie

Responses

The following errors downgrade the response from HTTPS to HTTP:

- 200 responses
- 30X responses
- 401 responses

HTTP 1.1 (HTTPS)

Response	Description
200	<p>We validate that no hyperlinks in the HTML for the web page downgrade the user inside the site and the domain of the site.</p> <p>We also validate and ensure the HTML of the webpage does not import resources (such as scripts and images) from outside the site using HTTP instead of HTTPS.</p> <p>The record is graded BAD if these resources are present.</p>
30x (301, 302, 307)	<p>We grade any HTTPS record that immediately downgrades the user to an HTTP connection using a redirect as BAD.</p>

HTTP 1.0 (HTTPS)

Response	Description
200	<p>We validate that no hyperlinks in the HTML for the web page downgrade the user inside the site and the domain of the site.</p> <p>We also validate and ensure the HTML of the webpage does not import resources (such as scripts and images) from outside the site using HTTP instead of HTTPS.</p> <p>The record is graded BAD if these resources are present.</p>
30x (302, 307)	<p>We grade HTTPS records that immediately downgrade the user to an HTTP connection using a redirect as BAD.</p>

Patching Cadence Risk Vector

This risk vector evaluates systems that are affected by software vulnerabilities (holes or bugs in software, hardware, or encryption methods that can be used by attackers to gain unauthorized access to systems and their data) and how quickly any issues are fixed.

Vulnerabilities

Publicly disclosed holes or bugs in software, hardware, or encryption methods. Information about Common Vulnerabilities and Exposures (CVE) is obtained from the [National Vulnerability Database \(NVD\)](#). A vulnerability might exist before its official announcement, but will not be evaluated and included in Patching Cadence risk vector until it's officially announced by the NVD.

Remediation

The process of updating software or taking other actions to ensure that the vulnerability is resolved ("patching"), so attackers can't use that channel for malicious purposes. Patches are applied either by automatically keeping operating systems and supporting libraries up-to-date or by manually configuring settings and modifying files until a patch is available.

The Patching Cadence letter grade is based on the time it takes an organization to remediate vulnerabilities (how quickly vulnerabilities were patched) and the prevalence of vulnerabilities within an organization's infrastructure. A vulnerability that's observed only once has less of an impact than a vulnerability that's observed over the span of several days.

Some vulnerabilities are more critical than others, and will carry greater weight than less critical vulnerabilities seen over the same time period. We follow the [Common Vulnerability Scoring System \(CVSS\)](#), which is a scoring system that uses various properties of the vulnerability for determining its level of severity.

Risks

Vulnerabilities can expose organizations to malicious attacks. With major vulnerabilities emerging at an increasing rate, reaction time is critical for reducing cyber risk.

Remediation



Refer to the Vulnerability Catalog and finding details, which includes the information your response teams will need to ensure that the vulnerability is eliminated from the affected systems.

- Conduct general housekeeping on company infrastructure. Keep software, hardware, operating systems, and supporting libraries up-to-date. Doing so can make it easier to patch systems in case vulnerabilities appear in the future.
- Ensure your operating systems and supporting libraries are up-to-date with the latest patches. Implement automatic updates for critical systems.
- Ensure new systems introduced into your corporate network are free of known vulnerabilities. Staying informed on the latest threats is a simple way to be aware of any possible risks your company could acquire when bringing any new devices onto your network.

- Find out how quickly your critical vendors are patching vulnerabilities. Your organization's security posture may be strong, but even one weak link in your supply chain can pose significant risk.

Impact

A vulnerability is considered to be “fixed” if it's observed to have been remediated (patched) or the service was observed to have been fully removed (taken offline). A service can be considered to be fixed after 60 days of no observations. The 60 days will not be included in the remediation time in these cases.

Field	Description	Value
Lifetime	<p>Once a vulnerability is fixed:</p> <ul style="list-style-type: none"> • Its impact on the letter grade of the particular risk vector improves linearly over time. It will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes (varies by risk vector). • The Patching Cadence letter grade will then reach a perfect value if all vulnerabilities and all Patching Cadence records are remediated and completes their lifetimes (300 days). 	300 Days
Letter Grade in the Absence of Records	The rating is positively impacted if there are no records for this risk vector.	 – “A” Letter Grade
Scan Frequency	<p>A check for changes is initiated, e.g., new Diligence records or an existing record was fixed.</p> <div style="background-color: #e0e0e0; padding: 5px; border: 1px solid #ccc;">  Findings are scanned at various intervals. At a maximum, they are scanned every 30 days. However, many unresolved findings are scanned weekly. </div>	30 Days
Refresh Processing	The processing time for a manually initiated scan.	Not Available
Grace Period	The time before a recognized record starts to impact ratings.	Impact is immediate. If all vulnerabilities are fixed and all Diligence records complete their

		lifetimes, the grade of this risk vector improves linearly over the lifetime of this risk vector (300 days).
Weight	Out of 35% in Diligence.	2%

Insecure Systems Risk Vector

This risk vector assesses endpoints (which can be any computer, server, device, system, or appliance with internet access) that are communicating with an unintended destination. The software of these endpoints may be outdated, tampered, or misconfigured. A system is classified as “insecure” when these endpoints try to communicate with a web domain that doesn’t yet exist or isn’t registered to anyone. This can happen for a few reasons:

- The device manufacturers/developers stopped supporting their product. The original domains that were registered have since become “abandoned” (the domain has not been renewed).
- A device has been purposely tampered with or is mis-configured. These devices are trying to reach out to unregistered/misnamed domains for software updates or other communications.

Some examples include mobile devices on debug or root mode that are reaching for rogue application content or abandoned applications fetching server configurations.

The Insecure Systems risk vector assessment is based on the supported/unsupported status and the level of risk that has been introduced to an organization.

Types of Insecure Systems

Category	Explanation of Risks	Examples of Systems in this Category
Debug Firmware Detected	<p>Explanation: Systems in this category are mobile devices that have rootkit capabilities disguised as a debug tool, and are reaching out to unregistered domains.</p> <p>[1][2] Risks:</p> <ul style="list-style-type: none">• Domain owners can push new firmware versions, hence controlling/hijacking the mobile device.• Firmware can send out unauthorized detailed information about the device.	Mobile Firmware
File Sharing	<p>Explanation: Systems in this category are reaching out to abandoned torrent tracker domains for information about files to download via BitTorrent. Learn more about File Sharing trackers.</p> <p>Risks:</p>	<ul style="list-style-type: none">• Expired Torrent Tracker• Gnutella Domains

	<ul style="list-style-type: none"> ● Attackers can set up false trackers and inject false information. ● Trackers can instruct clients to fetch files from an arbitrary list of systems, with false or dangerous content. 	
Proxy Configurations	<p>Explanation: Systems in this category are using an abandoned domain for proxy configuration. [1][2]</p> <p>Risks:</p> <ul style="list-style-type: none"> ● Domain owners can control browser navigation when proxies are used. ● Expired internal domains may have other severe implications. 	Misconfigured Proxy Domains
NetBios	<p>Explanation: Systems in this category are reaching out to Windows NetBios networks via an abandoned domain. [1][2][3]</p> <p>Risks:</p> <ul style="list-style-type: none"> ● Windows/NetBios connections represent a vulnerability because the NetBios protocol has known security vulnerabilities and is a common attack target. ● Domain owners can interact with endpoints, potentially hijacking Windows Challenge/Response (NTLM) authentication credentials. 	Windows NetBios
Abandoned Software	<p>Explanation: Systems in this category have applications which are either no longer maintained (the software has been “abandoned”* by its developers) or are communicating to the wrong servers; in either case, there is software present that is reaching out to an unregistered domain.</p> <p>Risks:</p> <ul style="list-style-type: none"> ● The app sends detailed information regarding how the device is being used, which could be used by attackers to gain access to the device. ● Domain owners could potentially leverage app functionalities to exfiltrate more information or gain a certain level of control over the device. 	<ul style="list-style-type: none"> ● Go Contacts Pro ● Auto Words With Friends Cheats ● Itiva Internet Accelerator


<p>IPTV</p>	<p>Explanation: Systems in this category are smart TV systems and other media systems that are reaching out to abandoned domains*.</p> <p>Risks: Endpoint** is reaching out to unused IPTV platform related services, which may allow attackers to capture endpoint data.</p>	<ul style="list-style-type: none"> ● Abandoned IPTV platform. ● Abandoned live TV add-on. ● Abandoned media hub. ● Abandoned swarmcast media.
<p>Remote Management</p>	<p>Explanation: Systems in this category involve either software that is responsible for automatically providing updates, or network or other hardware used in business environments, that is reaching out to abandoned domains*.</p> <p>Risks:</p> <ul style="list-style-type: none"> ● Attackers can potentially interact with endpoint** devices, simulating the endpoint management solution. ● Endpoints will not be able to install security and firmware updates, since they cannot reach the intended service, and may remain vulnerable to a number of attacks. 	<ul style="list-style-type: none"> ● Symantec Patch Management ● McAfee Corporate Antivirus ● McAfee ePolicy Orchestrator ● Microsoft Server Update Services ● Symantec Endpoint Protection Manager ● Honeywell HVAC Controllers ● My DLink Service ● TR-069 Protocol ● Citrix Receiver PN Agent
<p>LDAP</p>	<p>Explanation: Systems in this category have Lightweight Directory Access Protocol (LDAP) services running, which are used to manage information about an organization's employees, systems, and applications in the network; these services are reaching out to abandoned domains*.</p> <p>Risks: Attackers that hijack the abandoned domains may be able to interact with endpoints**, and obtain sensitive information.</p>	<p>Expired Windows LDAP Domains</p>
<p>SMB</p>	<p>Explanation: Systems in this category are reaching out to Windows NetBios networks via abandoned domains*.</p> <p>[1][2][3]</p> <p>Risks:</p> <ul style="list-style-type: none"> ● Windows/ NetBios connections represent a vulnerability because the NetBios protocol has known security vulnerabilities and is a common attack target. 	

	<ul style="list-style-type: none"> Domain owners can interact with endpoints**, potentially hijacking Windows Challenge/Response (NTLM) authentication credentials. 	
--	--	--

* “Abandoned domains” are no longer registered to anyone. They may have been abandoned if the manufacturer/developer shut down or it slipped the domain owner's attention.

** “Endpoints” refer to desktop computers, servers, or handheld devices that have internet access.

Impact

Field	Description	Value
Lifetime	The letter grade will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	60 Days
Letter Grade in the Absence of Records	The rating is positively impacted if there are no records for this risk vector.	 - “A” Letter Grade
Scan Frequency	A check for observations is initiated, e.g., newly observed Diligence records or an existing record was remediated.	Daily
Refresh Processing	The processing time for a manually initiated scan.	Not Available
Grace Period	The time before a recognized record starts to impact ratings.	New records immediately impact the grade.
Weight	Out of 35% in Diligence.	1%

Evaluation

Insecure Systems records are evaluated as NEUTRAL, WARN, or BAD. An overall letter grade is calculated, using the evaluations of individual records.

Software versions that cannot be determined or are unsupported, but still receive security fixes are evaluated as “NEUTRAL.” These items do not affect the Insecure Systems grade, but should be resolved.

Server Software Risk Vector

This risk vector helps track security problems introduced by server software that is no longer supported. Supported software versions receive attention from the software development team and vendor when bugs or vulnerabilities are discovered.

This can be used to create a rich picture about the software used by an organization. This makes it simple to maintain a robust, up-to-date array of server software applications in an organization's IT infrastructure.

Server Software includes support for the following software packages:

- [Microsoft IIS](#)
- [Apache HTTP Server Project](#)
- [PHP](#)
- [OpenSSH](#)
- [Wordpress](#)
- [Boa Webserver](#)
- [cPanel](#)
- [EmbedThis](#)
- [Kerio Connect](#)
- [MS Exchange](#)
- [MS SQL Server](#)
- [MS Windows Server](#)
- [serv-U](#)
- [Webmin](#)

Supported Versus Unsupported

Supported

Software vendors typically issue new versions of their software that address a number of bugs, vulnerabilities, or feature requests. Supported software versions receive attention from the development team and vendor when bugs or vulnerabilities are discovered.

There may be several concurrently supported versions for any server software. This is the typical process since customers and users may have operational requirements that prevent them from upgrading to the most recent version.

Example: Ubuntu Linux generally maintains multiple releases simultaneously. These releases often use different versions of the same software package.

The supported versions depend on the operating system in the server that's currently in use. Some operating system distributions may also have their own customized versions of popular server software.

Support Extensions

The general support life cycle of some software products are split into two periods – the first half with “mainstream support,” followed by the second half with “extended support.” After the extended support period, “Extended Security Updates (ESU)” might be offered [\[1\]](#).

Extended support and ESU are taken into consideration when determining if software is supported.

Unsupported


Unsupported software versions are marked by BitSight when they have been replaced by newer versions and are stated by the software vendor as deprecated or obsolete.

Assessment

Server Software letter grades are provided based on if the software is supported or not.

We cannot make any special exemptions with regards to the impact of this risk vector if an organization's business requirements depend on outdated or insecure server software applications. Please contact [BitSight Support](#) if you would like to discuss your Server Software records.

Impact

Field	Description	Value
Lifetime	The letter grade will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	60 Days
Letter Grade in the Absence of Records	The use of server software is not required to improve an organization's cyber security posture. Therefore, there's no penalty or negative impact to the rating in the absence of Server Software records.	 – "A" Letter Grade
Scan Frequency	A check for observations is initiated, e.g., newly observed Diligence records or an existing record was remediated.	8 Days
Refresh Processing	The processing time for a manually initiated scan.	2-3 Business Days
Grace Period	The time before a recognized record starts to impact ratings.	<ul style="list-style-type: none"> • New records immediately impact the grade. • Updated records won't necessarily improve the grade. • All BAD and WARN records will stop impacting the grade after the last observation, as it completes its lifetime (60 days).
Weight	Out of 35% in Diligence.	2%

Evaluation

Server Software records are evaluated as GOOD, NEUTRAL, or BAD based on the supported/unsupported status of an organization's server software.

GOOD

We can verify that the installed software is up-to-date or that it has the latest OS distribution-specific patches applied.

Backported Security Fixes

If server software that normally appears out-of-date receives backported security fixes, the software is graded as “GOOD.”

This occurs when software vendors still distribute updates (patches) for old software versions that are technically unsupported or when operating system distribution developers create patches for third-party software (Ubuntu developers update the Ubuntu version of OpenSSH) as a courtesy. They essentially duplicate security fixes from supported software versions and port them to the unsupported software.

NEUTRAL

If the software version status cannot be determined or is unsupported but still receive security fixes, they are evaluated as “NEUTRAL.” These do not impact the Server Software risk vector grade. Remediation is unnecessary in these cases.

- Not enough information to determine if the software version is supported.
- Not enough information to determine if the latest OS-specific patches are installed.
- Marked as unsupported, but still receives security fixes.

BAD

These items impact an organization's Server Software risk vector grade and BitSight Security Rating.

- The software version is unsupported, or
- The software does not have the latest OS-specific patches applied.

Software versions that are no longer supported are evaluated as “WARN” for a grace period of 28 days. After 28 days, records are evaluated as “BAD.”

Desktop Software Risk Vector

The Desktop Software risk vector assesses the supported or unsupported status of the software version. The use of desktop software is not required to improve an organization's cyber security posture. The version information of laptop and desktop software are compared with the latest and currently available software versions to determine if the device software is supported or out-of-date.

Desktop devices are laptops, servers, and other non-tablet, non-phone computers in a company's network that access the Internet. The outgoing communications from desktop devices includes metadata about the device's operating system and browser version.

Assessed Desktop Browsers

- Chrome
- Edge
- Firefox
- IE
- Safari

All other browsers are graded as “Neutral.”

Graded Desktop Operating Systems

- Chrome OS
- Mac OS X
- Windows: ME, NT, NT 4.0, Vista, XP, 95, 98, 7, 8, 8.1, 10, 2000

All other operating systems are graded as “Neutral,” including the following:

- Debian
- Fedora
- FreeBSD
- Linux
- NetBSD
- OpenBSD
- Slackware
- Ubuntu

Risks

Newer versions of operating systems and web browsers typically fix stability issues, bugs, and vulnerabilities that existed in older versions. Bad actors frequently exploit known bugs in older software versions to steal information or run malicious software. The use of unsupported operating systems and browsers is correlated with the presence of a high number of malware infections and an increased likelihood of breach.

- If there are unsupported desktop devices in an organization's network, there is a greater risk of:
 - System failure (vendor devices are not being maintained).
 - Disruption of business continuity.
 - Attackers may be able to use unpatched vulnerabilities to gain system access.

- Connecting a personal device to a corporate network infrastructure adds a potential surface of attack for a threat actor to gain access to company data and sensitive information.

Remediation

- Search and identify unsupported desktop software, and then update the software to the latest version.
- Set up auto-update methods for critical desktop software.
- Insufficient information prevents BitSight from identifying unsupported software. The use of software device management systems is recommended, along with integrating human processes that ensures systems in the organization are patched and the software is up-to-date.

Impact

Field	Description	Values
Lifetime	The letter grade will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	65 Days
Letter Grade in the Absence of Records	The absence of records for this risk vector does not negatively impact the rating. The impact of this grade towards the rating is equivalent to an A.	N/A – Not Applicable
Update Frequency	A check for observations is initiated, e.g., newly observed Diligence records.	1 Week
Refresh Processing	The processing time for a manually initiated scan.	Not Available
Grace Period	An unsupported piece of software begins to impact the grade 28 days after it officially becomes unsupported.	28 Days
Weight	Out of 35% in Diligence.	1.5%

Evaluation

Desktop Software records are evaluated as GOOD, FAIR, NEUTRAL, WARN, or BAD.

- **GOOD:** The version is supported.
- **FAIR:** The version has been unsupported for less than 4 weeks.
- **WARN:** The version has been unsupported for less than 52 weeks.
- **BAD:** The version has been unsupported for over 52 weeks.

The general support life cycle of some products is split into two periods – the first half with “Mainstream Support,” followed by the second half with “Extended Software Support (ESU).” This currently applies within the BitSight platform to Microsoft products.



Microsoft is the first program to be considered with ESU within the BitSight platform. These programs do not include all security fixes and upgrades.

Records of software with ESU are graded in the following manner:

- **GOOD:** From the date of release to the End-of-Life (EOL).
- **FAIR:** The first and second years of ESU.
- **WARN:** The third through fifth years of ESU (if available).
- **BAD:** The end of ESU.

The operating system (OS) and browser are graded independently from one another. Record evaluations represent the calculated combination of the OS and browser.

- **Undetermined:** If there's no version available, if the record cannot be identified, or if both the OS and browser records are unknown; the record is evaluated as "NEUTRAL."
- **Unknown:** If either the OS or browser has been graded and the other is unknown, the record is evaluated as the given grade.

Message	Description	Remediation Instructions	Evaluations (OS + Browser)
Neutral Operating System and Unknown Browser	Neither the browser version nor the operating system version could be determined.	If browser and operating system version obfuscation is intentional, ensure the organization has an update strategy in place for browsers and operating systems.	NEUTRAL + NEUTRAL (Unknown) = NEUTRAL
Unknown Operating System and Browser	The browser and operating system could not be recognized.	If browser and operating system version obfuscation is intentional, ensure the organization has an update strategy in place for browsers and operating systems.	NEUTRAL (Unknown) + NEUTRAL = NEUTRAL
Unknown Operating System and Supported Browser	The operating system details could not be recognized, but the browser is supported.	If operating system version obfuscation is intentional, for which there is no grade penalty, ensure the organization has an operating system update strategy in place.	NEUTRAL (Unknown) + GOOD = GOOD
Unknown Operating System and Unsupported Browser	The browser and the operating system are both unsupported.	Ensure the latest version of the operating system is installed, and after that, install the latest supported version of the desired browser.	NEUTRAL (Unknown) + FAIR = FAIR
			NEUTRAL (Unknown) + WARN = WARN
			NEUTRAL (Unknown) + BAD = BAD

Supported Operating System and Unknown Browser	The operating system is supported, but the browser could not be recognized.	If browser version obfuscation is not intentional, ensure that end-users are using approved mobile applications, in order to be able to analyze the supported (or unsupported) status of those applications.	GOOD + NEUTRAL (Unknown) = GOOD
Unsupported Operating System and Unknown Browser	The operating system is not supported, and browser information could not be determined.	Upgrade the operating system to the latest available version.	FAIR + NEUTRAL (Unknown) = FAIR
			WARN + NEUTRAL (Unknown) = WARN
			BAD + NEUTRAL (Unknown) = BAD
Neutral Operating System and Supported Browser	The browser is supported, and the operating system version could not be determined.	If operating system version obfuscation is intentional, for which there is no grade penalty, ensure the organization has an operating system update strategy in place.	NEUTRAL (Undetermined) + GOOD = GOOD
Unknown Browser and Operating System	The browser and operating system could not be recognized.	If browser and operating system version obfuscation is intentional, ensure the organization has an update strategy in place for browsers and operating systems.	NEUTRAL (Unknown) + NEUTRAL (Unknown) = NEUTRAL
Supported Operating System and Unsupported Browser	The browser is not supported, but the operating system is.	Ensure the latest version of the browser, for that operating system, is installed.	GOOD + FAIR = FAIR
			GOOD + WARN = WARN
			GOOD + BAD = BAD
Unsupported Operating System and Supported Browser	The operating system is not supported, though the browser is the latest supported version for that OS.	Ensure the latest version of the operating system is installed, and after that, install the latest supported version of the desired browser.	FAIR + GOOD = FAIR
			WARN + GOOD = WARN
			BAD + GOOD = BAD
Unsupported Operating	The browser and the operating	Ensure the latest version of the operating system is installed, and after	FAIR + WARN = WARN

System and Browser	system are both unsupported.	that, install the latest supported version of the desired browser.	FAIR + BAD = BAD
			WARN + FAIR = WARN
			WARN + BAD = BAD
			BAD + FAIR = BAD
			BAD + WARN = BAD
Supported Operating System and Browser	The detected browser and operating system are both supported.		GOOD + GOOD = GOOD
Neutral Operating System and Unsupported Browser	The browser is not supported, and the operating system version could not be determined.	Ensure the latest version of the browser, for that operating system, is installed.	NEUTRAL (Undetermined) + FAIR = FAIR
			NEUTRAL (Undetermined) + WARN = WARN
			NEUTRAL (Undetermined) + BAD = BAD

Mobile Software Risk Vector

The Mobile Software risk vector assesses the supported or unsupported status of the software version. The use of mobile software is not required to improve an organization's cyber security posture. The version information of mobile device operating systems and browsers are compared with the latest and currently available software versions to determine if the device software is supported or out-of-date.

Mobile devices are smartphones and tablets in a company's network that access the Internet. Outgoing communications from mobile devices include metadata about the device's operating system, device description, browser version, and description of applications.

Risks

Newer versions of operating systems and web browsers typically fix stability issues, bugs, and vulnerabilities that existed in older versions. Bad actors frequently exploit known bugs in older software versions to steal information or run malicious software. The use of unsupported operating systems and browsers is correlated with the presence of a high number of malware infections and an increased likelihood of breach.

- If there are unsupported mobile devices in an organization's network, there is a greater risk of:
 - System failure (vendor devices are not being maintained).
 - Disruption of business continuity.
 - Attackers may be able to use unpatched vulnerabilities to gain system access.
- Connecting a personal device to a corporate network infrastructure adds a potential surface of attack for a threat actor to gain access to company data and sensitive information.

Remediation

- Search and identify unsupported mobile software and then update the software to the latest version.
- Set up auto-update methods for critical mobile software.
- Insufficient information prevents BitSight from identifying unsupported software. The use of mobile device management (MDM) systems is recommended, along with integrating human processes that ensures systems in the organization are patched and the software is up-to-date.


Impact

Field	Description	Values
Lifetime	The letter grade will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	65 Days
Letter Grade in the Absence of Records	The absence of records for this risk vector does not negatively impact the rating. The impact of this grade towards the rating is equivalent to an A.	(N/A) – Not Applicable
Update Frequency	A check for observations is initiated, e.g., newly observed Diligence records.	1 Week
Refresh Processing	The processing time for a manually initiated scan.	Not Available
Grace Period	An unsupported piece of software begins to impact the grade 28 days after it officially becomes unsupported.	28 Days
Weight	Out of 35% in Diligence.	0.5%

Evaluation

Mobile Software records are evaluated as GOOD, FAIR, WARN, or BAD.

- **GOOD:** The version is supported.
- **FAIR:** The version has been unsupported for less than 4 weeks.
- **WARN:** The version has been unsupported for less than 52 weeks.
- **BAD:** The version has been unsupported for over 52 weeks.

 Software that becomes unsupported are given an additional grace period of up to 7 days and will be considered as “supported” during that time. This is because as the software reaches its end-of-life (EOL), an entire week of data on those versions is aggregated on a weekly basis (currently every Friday).

The general support life cycle of some products is split into two periods – the first half with “Mainstream Support,” followed by the second half with “Extended Software Support (ESU).” This currently applies within the BitSight platform to Microsoft products.

 Microsoft is the first program to be considered with ESU within the BitSight platform. These programs do not include all security fixes and upgrades.

Records of software with ESU are graded in the following manner:

- **GOOD:** From the date of release to the End-of-Life (EOL).
- **FAIR:** The first and second years of ESU.
- **WARN:** The third through fifth years of ESU (if available).
- **BAD:** The end of ESU.

Graded Mobile Browsers

- Android Browser
- BlackBerry WebKit
- Chrome Mobile iOS
- Chrome Mobile
- Firefox Mobile

All other browsers are graded as “Neutral.”

Graded Mobile Operating Systems

- Android
- iOS
- BlackBerry OS

All other operating systems are graded as “Neutral.”

DNSSEC Risk Vector

This risk vector determines if a company is using the DNSSEC protocol, which is a public key encryption that authenticates DNS servers, and then assesses the effectiveness of its configuration. The DNSSEC protocol protects against DNS spoofing, which involves diverting traffic to an attacker's computer, creating an opportunity for loss of confidentiality, data theft, etc.

For the DNSSEC Records risk vector, we look at a variety of criteria when determining the effectiveness of a Domain Name System Security Extensions (DNSSEC) record. Without DNSSEC configured, some data from the DNS server may not be secure.

Though DNSSEC is not standard in the industry, this risk vector is evaluated since DNSSEC protects DNS resolvers from receiving bad data by using public key encryption to sign domains or other zones to ensure authenticity of records. In short, this technology helps to protect everyday users from malicious redirects when looking up domain names. Refer to the list of [registrars that support end-user DNSSEC management](#).


Risks

Without DNSSEC, an organization's domain can more easily be taken over allowing an attacker to appear to be that organization online and perpetrate man-in-the-middle (MITM) attacks.

Remediation

- Set up DNSSEC for your domain, including generating the appropriate keys and updating DNS zone records.
- Generate a new Zone Signing Key using the RSA or DSA algorithm, with a key of 2048 bits or more.
- Download updated trust anchors and set them to be managed automatically.
- Add your DNSKEY to your DNS records through your registrar's management interface.

Impact

Field	Description	Value
Lifetime	The letter grade will reach a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	60 Days
Letter Grade in the Absence of Records	This risk vector does not currently affect security ratings. It is being evaluated for a period before being factored into BitSight Security Ratings.	 - "C (Beta)" Letter Grade
Scan Frequency	A check for observations is initiated, e.g., newly observed Diligence records or an existing record was remediated.	2 Weeks
Refresh Processing	The processing time for a manually initiated scan.	1 Business Day
Grace Period	The time before a recognized record starts to impact ratings.	Impact is immediate.
Weight	Out of 35% in Diligence.	Not Available

Evaluation

Each issue has a message shown in the platform as an individual entry, along with the associated IP address. For instance, “DSA public key is less than 2048 bits.” The text in the remediation column is also available in the platform. Remediation is guidance on how to resolve the issue so that it no longer adversely impacts the organization's BitSight Security Rating.

Record Grades

DNSSEC Records findings are evaluated as GOOD, NEUTRAL, WARN, or BAD.

GOOD

In order to be “GOOD,” the domain should have DNSSEC enabled and should be properly configured. The certificate must adhere to the following rules:

- It must be encrypted using a secure hash algorithm with a sufficiently long key.
- It must have a validated chain of trust.

NEUTRAL

These issues don't affect an organization's BitSight Security Rating.

WARN

The presence of these issues affects an organization's BitSight Security Rating. They should be remediated as soon as possible.

BAD

The presence of these issues affects an organization's BitSight Security Rating. They should be remediated as soon as possible.

Mobile Application Security Risk Vector

This risk vector analyzes the security aspects of an organization's mobile application offerings that are publicly available in official marketplaces, such as the Apple App Store and Google Play.

- It helps identify published applications that are at-risk, preventing the software from affecting its users and simultaneously reducing exposure to reputation damage.
 - Understand which, if any, applications at an insured present a risk for known vulnerabilities and other threats.
 - Verify quality and other contractual agreements with clients or vendors; for example, verify that a client has created secure software from a security standpoint.
- Mobile Application Security verifies the presence of support and email domains that should be provided in mobile applications. Mobile application offerings are evaluated to find security risks that can compromise end-users' devices and networks.

Only developer organizations that have mobile applications published in the US Android and iOS markets are evaluated for this risk vector. Therefore, apps published in other country marketplaces are not included for evaluation, i.e., Portugal, UK, Singapore, etc.

Mobile Application Security evaluates an organization's mobile application offerings in Android and iOS app stores to find security risks that can compromise end-users' devices and networks.

Criteria

Only developer organizations that have mobile applications published in the international Android and iOS markets will be evaluated for this risk vector. Therefore, apps published in a country marketplace are not included for evaluation, i.e., Portugal, UK, Singapore, etc.

If a third party developer is involved, please contact [BitSight Support](#) to learn more about Continuous Monitoring with the BitSight Security Ratings Platform.

Impact



This risk vector does not currently affect security ratings. It is being evaluated for a period before being factored into security ratings.

Field	Description	Value
Lifetime	Since apps cannot be verified to have been removed from or updated for all devices, a given app can impact the grade after the initial observation for the lifetime of this risk vector (1 year). This includes apps that are unlisted from the store.	1 Year
Letter Grade in the Absence of Records	Not all organizations have mobile application offerings.	- Not Applicable

Scan Frequency	A check for observations is initiated, e.g., newly observed Diligence records or an existing record was remediated.	2 Weeks
Refresh Processing	The processing time for a manually initiated scan.	3 Days
Grace Period	The time before a recognized record starts to be assessed.	Assessment is immediate. If a new app version is available, the new version replaces the previous record.
Weight	Out of 35% in Diligence.	Informational and does not currently affect security ratings.

Evaluation

A suite of security tests are performed on each mobile application. Any test failure is assigned a level of severity.

- Mobile Application Security records are given a record grade of GOOD, FAIR, NEUTRAL, WARN, or BAD. The severity level of the failed tests are used to determine the record grade of each individual application. We recommend prioritizing Mobile Application Security records that are graded as WARN and BAD.
- When calculating the Mobile Application Security risk vector letter grade, we only consider the severity of failed tests summed across all applications, and also the total number of applications that are published by the company.

Domain Squatting Risk Vector

The Domain Squatting risk vector detects the presence of domains named similarly to those that are owned and trademarked by an organization. Detection for these types of domains is based on information provided by DNS queries. It reveals if a company has registration coverage for domains that resemble their own primary/secondary domains, which render them most susceptible to these types of attacks.

Registering similarly named domains is called “domain squatting.” The Domain Squatting risk vector enables organizations to understand the breadth of domain names that are similar to their own and can be registered by attackers. We determine if domains are registered based on the information provided by DNS queries.

If new primary or secondary domains are added to a company, the data will be available the following week. If newly mapped companies are added to the BitSight inventory during the nightly data collection process, records will be available for those companies the following day.

Learn more about the [types of domain squatting](#).

Each domain variation is evaluated and grouped into one of the following states:

State	Description
Own Company	Indicates if the company who owns the target domain (appears in its domain map) registered the variation.
Another Company	Indicates if another company registered the variation. This assumes that organizations are not maliciously squatting. This helps resolve issues where Cosco legitimately has “cosco.com,” a domain variation of “cisco.com,” registered. This also captures cases where we have mapped Identity/Brand Protection companies and various companies in our inventory use these third-parties for brand protection. Example: SBC.com and ABC.com
Third Party	This domain is registered, but not by a known organization.
Not Registered	The domain is unregistered.

Impact

This risk vector is informational and does not currently affect BitSight Security Ratings.

Field	Description	Value
Lifetime	The letter grade reaches a perfect value if all records (associated with vulnerabilities) are remediated and they have completed their lifetimes.	Not Applicable
Letter Grade in the Absence of Records	This is an informational risk vector. It does not currently affect security ratings.	N/A – Not Applicable
Scan Frequency	A check for observations is initiated, e.g., newly observed Diligence records or an existing record was remediated.	8 Days
Refresh Processing	The processing time for a manually initiated scan.	Not Available
Grace Period	The time before a recognized record starts to impact ratings.	<ul style="list-style-type: none">Existing domains are impacted weekly.New domains are impacted the next day.
Weight	Out of 35% in Diligence.	Not Applicable

Types of Domain Squatting

The Domain Squatting risk vector is categorized into [Typographical Errors](#), [Spear Phishing](#), and [Bitsquatting Errors \(Bit-flip\)](#). These can be used as filters in the “Results by All Domains” view.

Typographical Errors

Users may mis-type the domain name. These domains are reached by simple typing mistakes and may also be used in spear phishing attacks.

Type	Description	Examples (saperix.com)
Insertion	Adding an extra letter to the domain name that's near an existing letter on the keyboard.	<ul style="list-style-type: none">asaperix.comsapericx.com
Omission	Dropping a character.	<ul style="list-style-type: none">sperix.com (saperix.com)saperx.com (saperix.com)
Repetition	Adding an extra letter that already exists.	<ul style="list-style-type: none">sapperix.comsaperrix.com

Replacement	Replacing a character with another one that's located near its placement on the keyboard.	<ul style="list-style-type: none"> ● saperic.com ● sapwrix.com
Subdomain	Misplacement of 1 of the periods in the domain.	<ul style="list-style-type: none"> ● s.aperix.com ● sa.aperix.com
Transposition	Flipping two characters.	<ul style="list-style-type: none"> ● spaerix.com ● sapreix.com
Vowel-swap	Replacing a vowel with a different one.	<ul style="list-style-type: none"> ● soperix.com ● sapirix.com
Various	Miscellaneous mistakes, including dropping the period from the fully qualified domain name.	<ul style="list-style-type: none"> ● wwwsaperix.com (www.saperix.com) ● www-saperix.com

Spear Phishing

The attacker's domain masquerades as being part of a legitimate organization, either directly or as a partner. These domain variations are registered by adversaries looking to commit spear phishing (email phishing) attacks on employees or customers of the targeted company.

Spear phishing attacks are targeted, proactive email campaigns against the user base (employees and customers) of an organization. They aim to fool users into opening an email attachment that are loaded with malware, get responses that contain sensitive information (e.g., login credentials, payment information, HR and tax documents), or redirect the user to a website that appears to be legitimate.

Type	Description	Examples (saperix.com)
Addition	Adding an arbitrary character to the end of the domain.	<ul style="list-style-type: none"> ● saperixj.com ● saperixb.com
Hyphenation	Inserting a hyphen between two characters.	<ul style="list-style-type: none"> ● sa-perix.com ● sap-erix.com
Homoglyph	Replacing characters that look like other characters, as in those frequently registered for spear-phishing attacks.	<ul style="list-style-type: none"> ● saper1x.com ● saperlx.com
TLD Variant	Using variants of the top-level domain (TLD).	<ul style="list-style-type: none"> ● example.country ● example.stream ● example.download

Bitsquatting Errors (Bit-flip)

Type	Description	Examples (saperix.com)
Bitsquatting	A bit is flipped for one of the characters.	<ul style="list-style-type: none">● saqerix.com● sbperix.com

File Sharing Risk Vector

This risk vector tracks the sharing of files, such as books, music, movies, TV shows, and applications. This includes files shared over the BitTorrent protocol or when observed on company infrastructure.

File Sharing focuses on the sharing of files using BitTorrent. It's tracked over the BitTorrent protocol when seen on company infrastructure and records the sharing of such files. There are other methods of sharing files, including popular methods using the Cloud and software products that include their own file sharing features.

Collected File Sharing Data

- Torrent name: “Van Halen Discography 320kbs,” “Adobe CS6 CRACKED,” “Diablo 3 No DRM,” etc.
- Torrent info hash: SHA-1 hash unique to every torrent.
- Event date: The entry observation date in the DHT, for that torrent, for that IP address.
- Peer IP: The IP of the torrent, as seen in the DHT.
- Content category: Sub-categories filter down into applications, books, games, movies, music, TV, other.

How File Sharing is Detected

Information is collected from BitSight data sources about the most popular files that are shared using BitTorrent, and then investigated for matches between the IP addresses of companies and the IP addresses collected from these sources.

Finding Details

When a match is detected -- file sharing activity is observed to be coming from a company's infrastructure using real data -- the activity is recorded as an event and placed into a category based on the torrent classification: books, music, movies, TV shows, and applications.

Information on every single active torrent is not collected.

Risks

There's no guarantee that content exchanged through BitTorrent has not been tampered with. This increases the risk of introducing malware to the system via malware or vulnerable software, such as unpatched and unregistered software.

[BitSight Blog, “Two Years Later, Still at Least Twice as Likely”](#)

Our research shows that the likelihood of experiencing a publicly disclosed data breach more than doubles if an organization has a File Sharing risk vector grade lower than an “A.”

The networks of 30,700 companies were observed across all industries and found 23% of organizations were using the BitTorrent protocol for peer to peer file sharing. Among these companies, 43% of torrented applications were also observed to contain malicious software.

- Despite matching content names or “official-sounding” titles, file sharing creates a risk of allowing malware to infect an organization's network.
- Systems damage, which can lead to a disruption of business continuity, potential loss of data, and theft of intellectual property.
- A company can encounter legal issues associated with using unlicensed software and media.

Remediation

Downloading content through approved channels, such as products directly from the software maker's corporate site or music through a mainstream music source, is the safest method for obtaining desired content because that content has been verified for authenticity.

- File Sharing events coming from your company's infrastructure can be found in the [Findings](#) tab. The [User Behavior Forensics](#) add-on package provides specific details about File Sharing events.
 - Use a firewall with Deep Packet Inspection to block torrent activity, as BitTorrent is difficult to block using standard port range rules.
-

Resources

- [BitSight](#), "[Is illegal file sharing occurring within your or your vendors' cyber ecosystem?](#)"
- [StackOverflow](#), "[How does DHT in torrents work?](#)"
- [BitTorrent.org](#), "[DHT Protocol](#)"

Exposed Credentials Risk Vector

This risk vector looks at verified breaches to indicate if the employees of a company had their information publicly disclosed and posted online as a result of a successful cyber attack on their company's third parties. Use this risk vector to identify breached sites and the types of information that were exposed ([disclosed fields](#)).

Risks

Exposure can be damaging to a company's systems and reputation. Attackers may gain access to user accounts either by directly hacking into an organization's database or by re-using credentials from a breach at an unrelated company, and then simply trying them all on an organization's web login page. Personally identifiable information that has been made public may decrease an employee's personal cybersecurity -- they may be more prone to identity theft or other fraud if enough sensitive details are made public.

If an employee reused their company username and password on a non-company website and those credentials are disclosed (and the passwords are visible or were guessed correctly) from the non-company website, an attacker could potentially gain access to an employee's corporate account.

Remediation

- Use Exposed Credentials as an opportunity to create or re-evaluate policies on information reuse, especially requirements concerning password reuse, password complexity, to address the potential risks associated with Exposed Credentials.
- Consider using 2-factor authentication as part of your organization's user account security strategy.

Finding Details

- **Observation Date:** The date of observation.
- **Exposure Date:** The date when records were exposed.
- **Breached Site:** The breached web site.
- **Domains:** The domains of this company that are affected.
- **Records:** The total number of the company's exposed records.

Disclosed Fields

The following table highlights the account details that are identified within those compromised sources:

Attribute Name	Description
Date of Birth	Demographic information about the owner of the disclosed account. Typically used by organizations for verification purposes.
Email Addresses	Any email addresses associated with the information in a disclosed user account, typically used for signup or notifications.
Gender	Demographic information about the owner of the disclosed user account.

Hashed Passwords	Passwords for this disclosed account were hashed (using SHA-1, for example), so that the original passwords were obscured, but not salted, making them vulnerable to dictionary attacks.
IP Addresses	The network addresses that the owner of the disclosed account used to sign in to and access the compromised source.
Known Languages	Demographic information about the owner of the disclosed account.
Name	Typically the real-world name of the owner of the disclosed account.
Password Hints	Any text stored by the user to help them remember what their password might be.
Personal Phone Number	Contact information for the owner of the disclosed account.
Physical Address	Typically the mailing address of the owner of the disclosed user account.
Physical Characteristics	Arbitrary text typically used on social networking or dating sites.
Plaintext Passwords	Passwords for this disclosed account were not stored in encrypted form.
Race	Demographic information about the owner of the disclosed account.
Relationship Status	Demographic information about the owner of the disclosed account.
Salted Hashed Passwords	Passwords for this disclosed account were hashed and a modifier used during hashing to make the stored password extremely difficult to guess.
Security Questions	User-supplied questions, and sometimes answers, for verification purposes.
Sexual Orientation	Demographic information about the owner of the disclosed account.
Social Network Accounts	Identifies on what other social network websites the owner of the disclosed account has additional accounts.
User Photograph	Typically an image of the owner of the disclosed account.
Username	Any user names associated with the information in a disclosed user account.
Work Phone Number	Contact information for the owner of the disclosed account.

Security Incidents Risk Vector

The Security Incidents risk vector involves a broad range of events related to the undesirable access of a company's data or resources, including personal health information, personally identifiable information, trade secrets, and intellectual property. They're grouped into the [Breach Security Incidents](#) and [General Security Incidents](#) categories.

Multiparty incidents, which are individual Security Incidents that impact multiple companies, can impact a company either directly as the original target or indirectly as a third party of the primarily targeted company.

CIA Triad

We also track a range of security events that contribute to any loss of information, known collectively as the "[CIA Triad](#)."

- **Confidentiality:** Indicates if access to sensitive data is restricted to the appropriate parties. Any unauthorized access due to a malicious attack or an internal error is considered a breach.
- **Integrity:** Indicates if data remains in its original form and is unaltered over its life cycle.
- **Availability:** Indicates if data is reliably accessible at all times.

Breach Security Incidents

Breach Security Incidents involve serious events that usually result in a successful cyberattack and/or data compromise by unauthorized individuals. Breach Security Incidents are ratings-impacting.

Incident Type	Description
Crimeware	An instance of malware installed for the purpose of acquiring unauthorized data or assets.
Espionage	An incident of unauthorized network or system access exhibiting the motive of state-sponsored or industrial espionage, where trade secrets or IP are frequently targeted.
Intrusion	Unauthorized access which does not involve exfiltration of records or other resources.
Phishing	An attack in which fraudulent email is used to mimic the access of an authorized employee or legitimate contact.
Ransomware	An attack designed to block access to a computer system until a sum of money is paid.
Social Engineering	An attack which uses deception to trick individuals into divulging unauthorized information or access.
Web Apps	An incident in which a web application was the attack vector, including code level vulnerabilities in the application and thwarted authentication mechanisms.

General Security Incidents

General Security Incidents involves other kinds of security events that may still affect security ratings, such as employee error or misconduct. General Security Incidents are considered more

severe than Other Disclosures. Some categories of General Security Incidents are ratings-impacting, while others are informational only and do not impact the rating.

Incident Type	Description
Account Takeover (Employee)	An attacker gains unauthorized access into a service through the use of employee's account credentials.
Account Takeover (User)	An attacker gains unauthorized access into a service through the use of a user's account credentials.
DNS Incident ^[1]	<p>An organization lost control or never had control of one of the associated assets, as defined by the DNS record^[2].</p> <p>Examples of poor DNS security practices:</p> <ul style="list-style-type: none"> • Using a stale DNS record. • Internally configuring publicly registrable domains (such as from an active directory), but not actually owning the domain.
Error	An incident involving unintentional actions that directly compromise a sensitive asset.
Internal Incident	An incident discovered by the company in question and remediated with no apparent compromise.
Lost/Stolen Asset	An incident where an information asset went missing, whether through misplacement or malice.
Lost/Stolen Asset (Encrypted)	An incident where an encrypted asset went missing, whether through misplacement or malice, with no evidence of encryption compromise.
Other Incident	A security incident that does not fall into one of the other categories.
Point of Sale (PoS)	Remote attacks against the environments where retail transactions are conducted, specifically where purchases are made.
Privilege Abuse	An unapproved or malicious use of organizational resources beyond what is authorized.
Unknown	A security incident where certain classification details pertaining to the event are unknown.
Unsecured Database	A database is left unsecured due to error and the data is accessible by third parties.

References

1. [Hackerone, "A Guide to Subdomain Takeovers"](#)
2. [The Register, "DNS entries left pointing to Azure-hosted server names snatched by miscreants for mischief"](#)

Other Disclosures Risk Vector

The Other Disclosures risk vector includes other kinds of publicly disclosed events. It's considered to be the least severe among the Public Disclosures risk vectors. Its impact to business continuity is minimal if they were to occur. Therefore, this risk vector is informational and does not currently affect BitSight Security Ratings.

Type	Description
ATM/Skimmer	A physical attack involving unauthorized access to an ATM, or the use of a skimming device to gather data from payment cards.
DoS	An attack intended to compromise the availability of networks and systems.
Other Disclosure	A disclosure that does not fall into one of the other categories.