The Economic Impact of Machine Identity Breaches

February 2020

AIR
A Verisk Business

VENAFI®

Copyright

Trademarks

Contact Information

If you have any questions regarding this document, contact:

AIR Worldwide Corporation
131 Dartmouth Street
Boston, MA 02116-5134
USA

Tel: (617) 267-6645
Fax: (617) 267-8284

Venafi
175 E 400, Suite 300
Salt Lake City, Utah 84111
USA

Tel: (801) 676-6900

Table of Contents

Executive Summary

Machines control the flow of our most sensitive data, help shape innovation and are fundamental to the way every business operates. But the way in which machines authorize machine-to-machine communication and the data flowing through them makes them a primary security risk for organizations. The rapidly growing number of machines on enterprise networks, the speed at which these machines are being created and changed, and the varied types of machines that need to communicate securely are creating a new and rapidly expanding attack surface. Cybercriminals routinely target machine identities because they are often poorly protected. Once compromised, machine identities can be powerful tools for attackers, allowing them to hide malicious activity, evade security controls and steal a wide range of sensitive data.

To quantify the cost of machine identity risks, AIR Worldwide and Venafi collaborated on this white paper, which evaluates the current cost of machine identity breaches.

Key Findings: Economic Impacts of Unprotected Machine Identities

- **Annual U.S. economic losses is USD 15.4 to 21.5 billion**
  - This estimate of annual U.S. economic losses is due to the poor protection of machine identities.
  - This assessed amount represents between 9% and 13% of total economic losses due to cyber events in the U.S., which are estimated at USD 163 billion.
  - Using worldwide estimates of economic losses due to cyber events and assuming the same 9% to 13% as above, it can be estimated that worldwide economic losses due to poor protection of machine identities are in the range of USD 51.5 and 71.9 billion.
- **Overall percentage of cyber losses for the largest companies is 14% to 25%**
  - The largest companies (with revenues of more than USD 2 billion) suffer the highest proportion of losses as a result of poor machine identity protection, which are estimated to be 14% to 25% of their overall cyber losses.
  - By comparison, an analogous proportion of cyber losses for companies in three revenue ranges below USD 2 billion are estimated to be between 6% and 16%.

Types and Uses of Machine Identities

Digital certificates and cryptographic keys – including SSL/TLS keys and certificates, SSH keys, and endpoint, user and code signing certificates – serve as machine identities. They are essential to a wide range of important security functions such as securing web traffic and transactions (including those involving sensitive or financial data), securing privileged access, authenticating software, and protecting communications on consumer devices. Every machine identity must be protected to effectively reduce risks.

Use of Machine Identities by Cyber Attackers

When machine identities are poorly managed and weakly protected, they become prime targets for cyber attackers who can use them to gain and maintain unauthorized access to network assets and data, impersonate trusted machines and applications, hide malicious activities and exfiltrate stolen data while remaining undetected. Any of these activities by cyber attackers can result in economic damage to organizations.

Basis for the Report's Economic Estimates

This report assesses U.S. economic losses that have occurred as a result of poorly protected machine identities. A range of estimates, representing higher and lower confidence that the losses are indeed due to mismanagement of machine identities are presented. These estimates are obtained by combining cyber event data sets with assessments upward of 100,000 firms' performance in various areas of cybersecurity. Security ratings are based on the evaluation of each organization's management of cybersecurity (e.g., proper configuration and management of SSL/TLS certificates); user behavior (e.g., use of file-sharing services/protocols such as torrent); and indicators of compromise (e.g., outgoing communications to botnet command and control servers). The methodology for this report takes factors such as company size and industry into consideration when estimating economic losses.

Data Sources Used for the Economic Estimates

- **Event data sets:** These data provide a list of (publicly reported) historical cyber events – such as breach/data compromise events and downtime events – and indicate the company name, industry sector, event categorization, brief event description and number of records lost (for data compromise events).
- **Firmographic data sets:** These data provide a complete list of U.S. businesses, along with *firmographic* information about each listed company – including company name, industry sector, employee count and revenue.
- **Technographic data sets:** These data provide a list of businesses, along with *technographic* information (i.e., information about used technologies, the cyber supply chain and management of computer assets) about each listed company – including company name, industry sector, employee count and security ratings.

With the three types of data sets above, estimates of losses caused by poorly protected machine identities were obtained as follows. First, event data sets and technographic data sets were combined to determine the cyber events that occurred when companies did not properly protect their machine identities. From this set of events, the proportion of events that were found to have been a result of poorly protected machine identities was calculated. Additionally, this data was combined with firmographic data sets to obtain estimates of how this proportion varies as a function of company size. Finally, loss estimates to the U.S. economy were derived by using these proportions in AIR's probabilistic cyber model, as described below.

AIR's Probabilistic Cyber Model

AIR's probabilistic data compromise model projects the likelihood of a data compromise of a specific magnitude affecting a single company. Generally speaking, factors influencing data compromise losses include company size by revenue, the number of lost records and industry. When individual company security ratings data is available, this technographic data is used to estimate a particular company's breach probability by running the ratings through a random forest machine-learning model. When technographic data is not available, the model calculates the probability of a breach as a function of revenue using industry-dependent curves. The computed probability, in this case, corresponds to the breach probability for a company with "average" security. Breach severity, as measured by the number of records lost, is simulated by industry-dependent probability distributions, along with revenue and industry-dependent caps on the maximum number of records lost. Finally, losses are simulated as a function of a company's industry, revenue and the (simulated) number of records lost.

Ramifications of These Findings

Organizations depend on secure machine-to-machine connections and communications, which rely on machine identities for authentication and encryption, for nearly every type of confidential business transaction. To ensure these machine identities stay secure, a strong machine identity protection program must be an essential part of every organization's cybersecurity program. This report quantifies the cost of failure, demonstrating that roughly USD 15 to 20 billion in losses to the U.S. economy could be eliminated through proper management and security of machine identities.

Although the focus of this report is on the U.S. economy, the same methodology could be applied to estimate losses enabled by mismanagement of machine identities in other countries, as well as the global economy. An estimate could be obtained by assuming that the same 9% to 13% proportion of economic losses due to cyber events that were enabled by poor protection of machine identities applies globally. According to a report by the Center for Strategic and International Studies (CSIS), the cost of cyber crime in North America is between USD 140 and 175 billion.[1] This is in comparison to a global estimate of between USD 445 and 608 billion. Scaling up our U.S. estimate of USD 15.4 to 21.5 billion therefore yields a global estimate of between USD 51.5 and 71.9 billion in losses to the global economy that could be eliminated through proper management of machine identities.

[1] Source: Center for Strategic and International Studies , Economic Impact of Cyber Crime – No Slowing Down, 2018, https://www.csis.org/analysis/economic-impact-cybercrime.

Methodology Overview

At a high level, the procedure for estimating losses consists of the following steps:

1. Joining the event data sets to the technographic data sets to obtain security posture information (i.e., security ratings) about the companies that suffered cyber events.
2. Defining combinations of security ratings and/or event types that are indicative of poor protection of machine identities.
3. For each defined combination of security ratings and/or event types, determining the subset of events where the impacted company satisfies the constraints of the given combination. These form the subset of events that are assessed to have been enabled by poor protection of machine identities.
4. Joining the event data sets to the firmographic data sets to determine, for each combination of industry and four revenue classes, what the probability is of a cyber event having been due to poor protection of machine identities.
5. Combining losses from AIR's probabilistic cyber model with the probabilities determined in the previous step to estimate economic losses that are assessed to have been caused by events enabled by poor protection of machine identities.

These steps will be described in greater detail in the remainder of this document. Prior to doing so, we provide more information on the technographic security ratings, so that the reader can properly understand the approach to assessing which events are deemed to be enabled by poor protection of machine identities.

Security Ratings

These data assess the security rating of more than 100,000 companies from an outside-in perspective. Examples of security rating indicators include:

- Patching cadence
- TLS/SSL certificates
- SPF (Sender Policy Framework)
- Botnet infections
- Spam propagation

The raw data used for these security ratings are obtained through various techniques, including spam traps and sinkholes. Spam traps use email addresses that have been purposely placed in email lists known to be consulted by spammers. Sinkholing is the practice (typically by cyber security researchers) of claiming ownership of domain names associated with malware, such as botnets, to determine who is communicating with the malicious domains. Outgoing communication to a domain associated with malware (e.g., a botnet's command and control server) is a strong signal that the source of the communication has been compromised by malware.

Measures for a variety of security ratings are obtained by aggregating the raw data, controlling for company size. Thus, a number of observations of "bad" indicators/behavior/events (what constitutes a bad indicator depends on the particular security rating) for a small company will be deemed worse than the same number of observations for a large company. The derivation of the ratings also includes an observation window—beyond which observations no longer contribute to the score—as well as a decay, so that more recent events have greater weight.

Determining Which Events Are Likely to Have Been Enabled by Poor Protection of Machine Identities

Ideally, the historical event sets would have highly detailed explanations describing not only what happened and what the consequences were, but also how it happened (e.g., if a vulnerability was exploited, noting which one). In practice, the event sets are gathered from public reports, such as news articles and 10K reports, and a detailed analysis of how a cyber event occurred is frequently not provided by the company suffering the cyber event. Although the cyber event data sets categorize events with labels such as Hack/Malware or Cyber Extortion, these labels are not specific enough to assess whether the event was somehow related to the quality of a company's management of machine identities.

Instead of relying solely on the information from the event sets, which is not adequate for the research described here, we examined companies' performance with respect to the following six security rating indicators:

- **Botnet Infections**: Measures the frequency of observations of a device in a company's network communicating with botnet command and control (C&C) servers
- **Malware Servers**: Measures the frequency of observations of a company's servers engaged in malicious activity, such as hosting fraudulent sites
- **Potentially Exploited**: Measures the frequency of observations of malware infections in the browsers used on a company's networks
- **TLS/SSL Certificates**: Assesses the use and strength of SSL (secure socket layer) and TLS (transport layer security, the successor to SSL) certificates. Penalizes companies for using expired or distrusted certificates, or weak (short) cryptographic keys

- **TLS/SSL Configurations**: Assesses how TLS/SSL is configured, penalizing misconfigurations that make servers vulnerable to attacks such as Heartbleed, or that do not support stronger encryption standards.
- **Web Application Headers**: Assesses how well the http(s) headers of web applications protect against classes of attacks such as man-in-the-middle attacks and cross-site scripting attacks.

Informally, the first three categories are evidence of existing compromise, whereas the latter three categories assess how well a company is protecting machine identities. These six indicators were deemed the most relevant to assessing protection of machine identities out of a larger set of approximately 20 rating indicators.

With the set of relevant security indicators identified, the next step was to determine which combinations of event types and/or performance in the respective rating vectors were indicative of an event that was enabled by poor protection of machine identities. Because the rating vectors do not have any “absolute” meaning, the quality of a company’s scores in the rating vectors was assessed on a *relative* basis, by comparing companies to similarly sized peers. Thus, the individual ratings were converted to percentiles by comparing the score of a given company to those of other companies of similar size, as measured by employee count. The normalization by company size was necessary because a particular rating might be among the best for a small company, but among the worst for a larger company (or vice-versa). The output of this process was a set of curves defining the scores at the 10th, 20th, 30th, etc., percentile levels as a function of employee count.

Defining the Cases

As stated above, six security rating indicators were used, which could be grouped into one set indicative of existing compromise, and another set indicative of proper protection of machine identities. We provide more information below.

Infected Machines:
Compromised systems are often used to distribute malware, infect other systems, and expand attacks. Indicators of *Botnet Infections*, *Malware Servers*, and indicators that systems are *Potentially Exploited*, such as communication attempts by unwanted applications, demonstrate that systems connected to the internet are likely infected and under control of malicious actors. Organizations that do not have control over machine identities and the encrypted tunnels they create may not be able to identify these compromises. Many organizations that suffer from infected machines lack the machine identity intelligence to understand which machines and connections should be trusted; they also may not have the ability to inspect encrypted traffic. These failures leave organizations blind to these infections and the resulting compromises.

Machine Identity Security and Proactive Protection:
Digitally transformed businesses must ensure privacy and authenticate every connection in data centers, the cloud, and across the internet. This requires higher than average use of *TLS Certificates* and the encryption of a much higher percentage of network traffic. Properly configured *Web Application Headers* indicate that systems are proactively secured against attacks. To mitigate attacks hiding in the increased level of encrypted traffic, threat protection systems need to be enabled. In addition, *TLS Configurations* must be correct in order to eliminate errors that might create vulnerabilities or errors such as certificate expiration–based outages. This requires that *TLS Configuration* be correct, and it also requires *TLS Certificate* lifecycle orchestration to make sure there are no unknown *TLS Certificates* and that *TLS Certificates* are provided to threat-protection systems to perform inspection of encrypted traffic. Without these machine identity security controls in place, organizations are blind to attacks that target these critical security assets.

Based on the above, a list of "cases" was defined, each constituting one combination of security ratings indicators and breach type from the event data sets. Table 1 lists these cases. We have used < or > to signify that a particular security rating is worse or better than average, and << or >> to signify that a particular security rating is much worse or much better than average. The terms much worse, worse, better, and much better than average are all defined in terms of percentiles. One percentile threshold was used for better and worse than average, and another threshold was used for much better and much worse than average.

As an example, if the threshold for better and worse than average was 30% and the threshold for much better and much worse than average was 10%, then an event would satisfy the constraints of Case 3b (see Table 1) if *each* of the following conditions is satisfied:

1. Either the Botnet Infections rating is in the *bottom* 30% (<) OR the Malware Systems rating is in the *bottom* 30% (<) OR the Potentially Exploited rating is in the *bottom* 30% (<) OR the breach type is "Web."
2. AND the TLS Certificates rating is in the *top* 10% (>>)
3. AND the TLS Configurations rating is in the *top* 10% (>>)
4. AND the Web Application Headers rating is in the *top* 30% (>).

Table 1. Case descriptions for assessing which events can be associated to mismanagement of machine identity

		At Least 1				And			
Case Description	**Case**	**Bots**	**Malware**	**Exploited**	**Breach Type**	**TLS Cert**	**TLS Conf**	**Web Header**	**Breach Type**
Encrypted Traffic Likely	1a	< Avg	< Avg	< Avg	Web	> Avg	> Avg		
Encrypted Traffic Likely	1b	< Avg	< Avg	< Avg	Web	> Avg	> Avg	> Avg	
Encrypted Traffic Likely	2a	< Avg	< Avg	< Avg	Web	> Avg	< Avg		
Encrypted Traffic High	2b	< Avg	< Avg	< Avg	Web	> Avg	< Avg	> Avg	
Encrypted Traffic High	3a	< Avg	< Avg	< Avg	Web	>> Avg	>> Avg		
Encrypted Traffic High	3b	< Avg	< Avg	< Avg	Web	>> Avg	>> Avg	> Avg	
Unmitigated DDOS Attack	4					>> Avg			Network / Website Disruption
Phishing Attack Likely	5					> Avg			Phishing
Phishing Attack High	6					>> Avg			Phishing
Chaotic Machine Identity Use Likely	7a					< Avg	< Avg		
Chaotic Machine Identity Use Likely	7b					< Avg	< Avg		Phishing *or* Web *or* Hack
Chaotic Machine Identity Use High	8a					<< Avg	<< Avg		
Chaotic Machine Identity Use High	8b					<< Avg	<< Avg		Phishing *or* Web *or* Hack
Chaotic Machine Identity Use High	9					<< Avg	<< Avg		Network / Website Disruption *or* IT – Config / Implement Errors

To obtain a range of estimated losses, we used two combinations of thresholds for the better/worse than average percentiles and the much better/much worse than average percentiles (see Table 2).

Table 2: Percentile combinations examined in associating events to cases

Threshold	Combination 1	Combination 2
Better/Worse than Average (Percentile 1)	20%	30%
Much Better/Much Worse than Average (Percentile 2)	10%	20%

Clearly, Combination 2 results in higher loss estimates than Combination 1, as the former is strictly more permissive in evaluating when a case's constraints are met. Consequently, we will often refer to Combination 1 as the *higher confidence* percentile combination, as we can be more confident that events meeting these criteria were enabled by poor protection of machine identities, and Combination 2 as the *lower confidence* percentile combination in the remainder of this document.

Estimating Losses

The 14 cases defined in the previous section allowed for the labeling of events in the event sets as either satisfying the constraints of cases or not. Given the assignment of events to cases, determining the probability that a cyber event was enabled by poor protection of machine identities is as straightforward as simply computing the proportion of events that are assigned to one of the cases. However, such a simple methodology does not account for differences in quality of security posture, which are correlated to industry or company size. To account for such differences, the set of events was joined to firmographic information, augmenting the events with information about the company's industry and revenue. With this information one can determine the proportion of cyber events that can be tied to poor protection of machine identities as a function of company industry and size.

These proportions were then used to obtain loss estimates by scaling AIR's company-by-company modeled cyber losses by the appropriate proportion for each company. These losses are given below. For the sake of comparison, reference losses are provided as well. These reference losses represent the average annual economic loss from all cyber events in the probabilistic model, i.e., including those *not* assessed to have been enabled by poor protection of machine identities. *The numbers in Table 3 are in USD millions.*

For each of the two percentile combinations, we provide overall losses as well as losses broken out by case and by each of the revenue classes (ranges of company revenues). The first set of losses is the overall losses.

Table 3. Total economic losses assessed to be due to mismanagement of machine identity, USD millions

Percentile Combination	Loss	Reference	Proportion
Higher Confidence	$15,366	$163,397	0.094
Lower Confidence	$21,489	$163,397	0.132

As Table 3 demonstrates, the model's estimated economic loss from cyber events in the U.S. is USD 163 billion. This represents a bit less than 1% of U.S. gross domestic product (GDP), which is estimated to be approximately USD 20.5 trillion (https://data.worldbank.org/indicator/NY.GDP.MKTP.CD, 2018). Of the estimated USD 163 billion, between 9% and 13% of losses are attributed to mismanagement of machine identity.

Next, we display losses by case. Because the cases are not mutually exclusive, we present two versions of the results. Table 4 is the *non-exclusive* version, in which we use the calculated proportions as they are, without making any correction for the fact that the cases are not mutually exclusive. Table 5 is the *exclusive* version, in which each event is assigned to one case. If an event satisfies the constraints of more than one case, then the event is assigned to the most specific case (ex: Case 1b is more specific than Case 1a because it has an additional constraint). If an event satisfies the constraints of multiple cases that have non-comparable constraints, then the event is assigned to each case with an equal weight that sums to 1. The impact is that losses are split between the cases. In both versions, the reference loss is the same USD 163 billion as above, and therefore is omitted from the tables. The listed proportion is relative to this loss.

Table 4. Economic losses assessed to be due to mismanagement of machine identity, broken out by case (exclusive version), USD millions

Percentile Combination	Case	Loss	Proportion
Higher Confidence	1a	$278	1.70E-03
Higher Confidence	1b	$114	7.01E-04
Higher Confidence	2a	$1,835	1.12E-02
Higher Confidence	2b	$7	4.01E-05
Higher Confidence	3a	$345	2.11E-03
Higher Confidence	3b	$197	1.21E-03
Higher Confidence	4	$416	2.55E-03
Higher Confidence	5	$229	1.40E-03
Higher Confidence	6	$697	4.27E-03
Higher Confidence	7a	$2,202	1.35E-02
Higher Confidence	7b	$2,216	1.36E-02
Higher Confidence	8a	$1,800	1.10E-02
Higher Confidence	8b	$4,189	2.56E-02
Higher Confidence	9	$840	5.14E-03
Lower Confidence	1a	$1,623	9.93E-03
Lower Confidence	1b	$1,248	7.64E-03
Lower Confidence	2a	$2,850	1.74E-02
Lower Confidence	2b	$40	2.48E-04
Lower Confidence	3a	$1,284	7.86E-03
Lower Confidence	3b	$844	5.17E-03
Lower Confidence	4	$438	2.68E-03
Lower Confidence	5	$424	2.59E-03
Lower Confidence	6	$704	4.31E-03
Lower Confidence	7a	$1,751	1.07E-02
Lower Confidence	7b	$1,204	7.37E-03
Lower Confidence	8a	$3,048	1.87E-02
Lower Confidence	8b	$5,177	3.17E-02
Lower Confidence	9	$853	5.22E-03

Table 5. Economic losses assessed to be due to mismanagement of machine identity, broken out by case (non-exclusive version), USD millions

Percentile Combination	Case	Loss	Proportion
Higher Confidence	1a	$840	5.14E-03
Higher Confidence	1b	$296	1.81E-03
Higher Confidence	2a	$1,551	9.49E-03
Higher Confidence	2b	$7	4.57E-05
Higher Confidence	3a	$505	3.09E-03
Higher Confidence	3b	$202	1.24E-03
Higher Confidence	4	$399	2.44E-03
Higher Confidence	5	$847	5.18E-03
Higher Confidence	6	$653	3.99E-03
Higher Confidence	7a	$9,322	5.71E-02
Higher Confidence	7b	$5,306	3.25E-02
Higher Confidence	8a	$5,705	3.49E-02
Higher Confidence	8b	$3,428	2.10E-02
Higher Confidence	9	$686	4.20E-03
Lower Confidence	1a	$5,106	3.12E-02
Lower Confidence	1b	$2,195	1.34E-02
Lower Confidence	2a	$3,059	1.87E-02
Lower Confidence	2b	$43	2.65E-04
Lower Confidence	3a	$2,273	1.39E-02
Lower Confidence	3b	$932	5.71E-03
Lower Confidence	4	$492	3.01E-03
Lower Confidence	5	$1,327	8.12E-03
Lower Confidence	6	$842	5.15E-03
Lower Confidence	7a	$12,449	7.62E-02
Lower Confidence	7b	$6,577	4.02E-02
Lower Confidence	8a	$9,680	5.92E-02
Lower Confidence	8b	$5,362	3.28E-02
Lower Confidence	9	$883	5.41E-03

Conclusions that can be reached from the above data include the following:

- A majority of the losses fall under cases 7a-9 (approx.. 73% at the higher confidence threshold, 56% at the lower confidence threshold). These are the cases where companies have poor management of TLS/SSL certificates.
- Cases 1a-3b have a much smaller proportion of the losses when using the higher confidence threshold (approx. 18%) than when using the lower confidence threshold (approx. 37%). In fact, these six cases account for almost two thirds of the increase in losses between the higher and lower confidence thresholds. The large increase in losses for these six cases is explained by the fact that these cases all require companies to have high security ratings in some categories and low ones in other categories. In practice, there is a high degree of correlation between the various categories, so such a combination is rare. These "good and bad" combinations become much more common at the lower confidence percentiles.
- The remaining cases (4-6) account for roughly the same proportion for both percentile combinations (9% for the higher confidence combination, 7% for the lower percentile combination). These are cases where a company has good management of TLS certificates, but nevertheless falls victim to a phishing attack or to a disruption of their website or network.

In Table 6 we display the breakdown of losses into four revenue classes. The revenue class bounds are given in USD millions.

Table 6. Economic losses assessed to be due to mismanagement of machine identity, broken out by revenue class, USD millions

Percentile Combination	Rev Class	Minimum Revenue	Maximum Revenue	Loss	Reference	Proportion
Higher Confidence	A	$2,000	$1,000,000	$470	$3,349	0.140
Higher Confidence	B	$50	$2,000	$491	$7,712	0.064
Higher Confidence	C	$10	$50	$3,284	$23,472	0.140
Higher Confidence	D	$0	$10	$11,122	$128,865	0.086
Lower Confidence	A	$2,000	$1,000,000	$826	$3,349	0.247
Lower Confidence	B	$50	$2,000	$971	$7,712	0.126
Lower Confidence	C	$10	$50	$3,649	$23,472	0.155
Lower Confidence	D	$0	$10	$16,043	$128,865	0.124

We first note that the vast majority of companies have a revenue of less than USD 10 million, so even though the average annual loss per company is much smaller for these than it is for, say, multibillion-dollar enterprises, the small companies contribute the majority of cyber losses. Interestingly, this trend is almost completely reversed when examining insured losses (not displayed here), because of the much higher take-up rates of cyber insurance for larger companies.

At the higher confidence percentile combination, there is little indication of any trend in revenue. However, at the lower confidence percentile combination (which is based on a greater amount of data because more events qualify), it is clear that the proportion of losses enabled by poor protection of machine identities is much higher for the largest companies than it is for smaller companies. One possible explanation for this is that the larger companies are targeted far more often, and they have larger numbers of machines, which makes them more vulnerable to attacks targeting machine identities.

About Venafi

Venafi is the cybersecurity market leader in machine identity protection, securing machine-to-machine connections and communications. Venafi protects machine identities by automating the management and security of cryptographic keys and digital certificates for SSL/TLS, SSH, mobile and code signing. Venafi provides the global visibility, intelligence and automation of machine identities across the extended enterprise—on premises, mobile, virtual, cloud and IoT— necessary to eliminate certificate outages and reduce critical security risks. For more information, visit www.venafi.com.

About AIR Worldwide

AIR Worldwide (AIR) provides risk modeling solutions that make individuals, businesses, and society more resilient to extreme events. In 1987, AIR Worldwide founded the catastrophe modeling industry and today models the risk from natural catastrophes, terrorism, pandemics, casualty catastrophes, and cyber incidents. Insurance, reinsurance, financial, corporate, and government clients rely on AIR's advanced science, software, and consulting services for catastrophe risk management, insurance-linked securities, site-specific engineering analyses, and agricultural risk management. AIR Worldwide, a Verisk (Nasdaq:VRSK) business, is headquartered in Boston, with additional offices in North America, Europe, and Asia. For more information, please visit www.air-worldwide.com.