The metrics come from a variety of industries and locations:

Sources of Metrics	
Industries	Locations
Defense/aerospace Energy/oil Finance/banking Government Insurance Manufacturing/industrial products Pharmaceutical Real estate management Retail Security services Shipping/logistics Telecom	United States Africa Australia/Asia Pacific Europe

The metrics are not presented as models of perfection. Rather, they are authentic examples that security professionals can follow, refine, or otherwise adapt when developing their own metrics.

A. Environmental Risk Metric

At a major insurance company headquartered in the Midwestern United States, the assistant vice president for corporate security uses an environmental risk metric to help the company decide where to place office facilities around the country. The metric, in use for 12 years, is designed to serve the risk management needs of the corporation.

The company owns or leases hundreds of facilities across the United States. Corporate security regularly collects a suite of data, assigns weights to various factors, and develops a numeric score that places each facility into a low, medium, or high category of risk. For each risk category, written policy specifies a collection of security measures that should be in place at the site. Exceptions can be granted, but the systematic approach results in uniformity and in efficiency in decision-making and security systems contracting. Most important, the *metrics-based approach helps senior management understand the level of risk in site selection and make informed decisions on risk management. In addition, over time, the metrics have steered the corporation toward having a smaller percentage of its locations in high-risk sites.*

The formula for the ongoing risk assessment metric creates a score from four elements:

1. CAP Index Score (local risk analysis) [CAP Index is a commercial provider of crime risk forecasting. CAP stands for Crimes Against Persons and Crimes Against Property.]

The average national crime rating score through CAP is 100. CAP is valued as follows: 1 – CAP score of 100 or lower; 2 – CAP score of 101 to 200; 3 – CAP score of 201 to 300; 4 – CAP score of 301 to 400; 5 – CAP score of 401 to 500; 6 – CAP score of 501 to 600.

Locations with a score of 601 or more will not be considered as a location for an office.

2. Type of environment

1 – Non-critical: storage, empty space, surplus equipment. Locations that, if rendered inoperable, would have little or no negative impact on business processes. 3 – Sensitive: administrative, claims, trial office, sales office or other public contact. Locations that, if rendered inoperable, could have their work transferred to another location with little impact to the business. 5 – Mission critical: IT/data center, call center, headquarters. Locations that, if rendered inoperable, would negatively impact the business for an extended period.

3. Sensitivity of the asset

1 – Low: Nothing of irreplaceable value including non-identifying records, furniture, low value equipment, perishable supplies, surplus assets. Facility may not be identified/branded as a corporate asset. 3 – Medium: Valuable equipment, associates, personally identifying records. Facility is branded as a corporate asset. 5 - High: Critical information/data, leadership associates, board members, cash/cash equivalents and critical infrastructure. Facility is identified as an integral part of the corporation, branded and well known in the community.

4. Occupancy type

1 – Unoccupied space; 2 – Mixed tenant space; 3 – Sole tenant

The risk levels are then defined by totaling the preceding scores: Low-risk location = 4 to 9 points; Medium-risk location = 10 to 15 points; High-risk location = 16 to 19 points.

The metric is presented quarterly to the corporate risk committee, and corporate policy defines the security measures required at each level of risk.

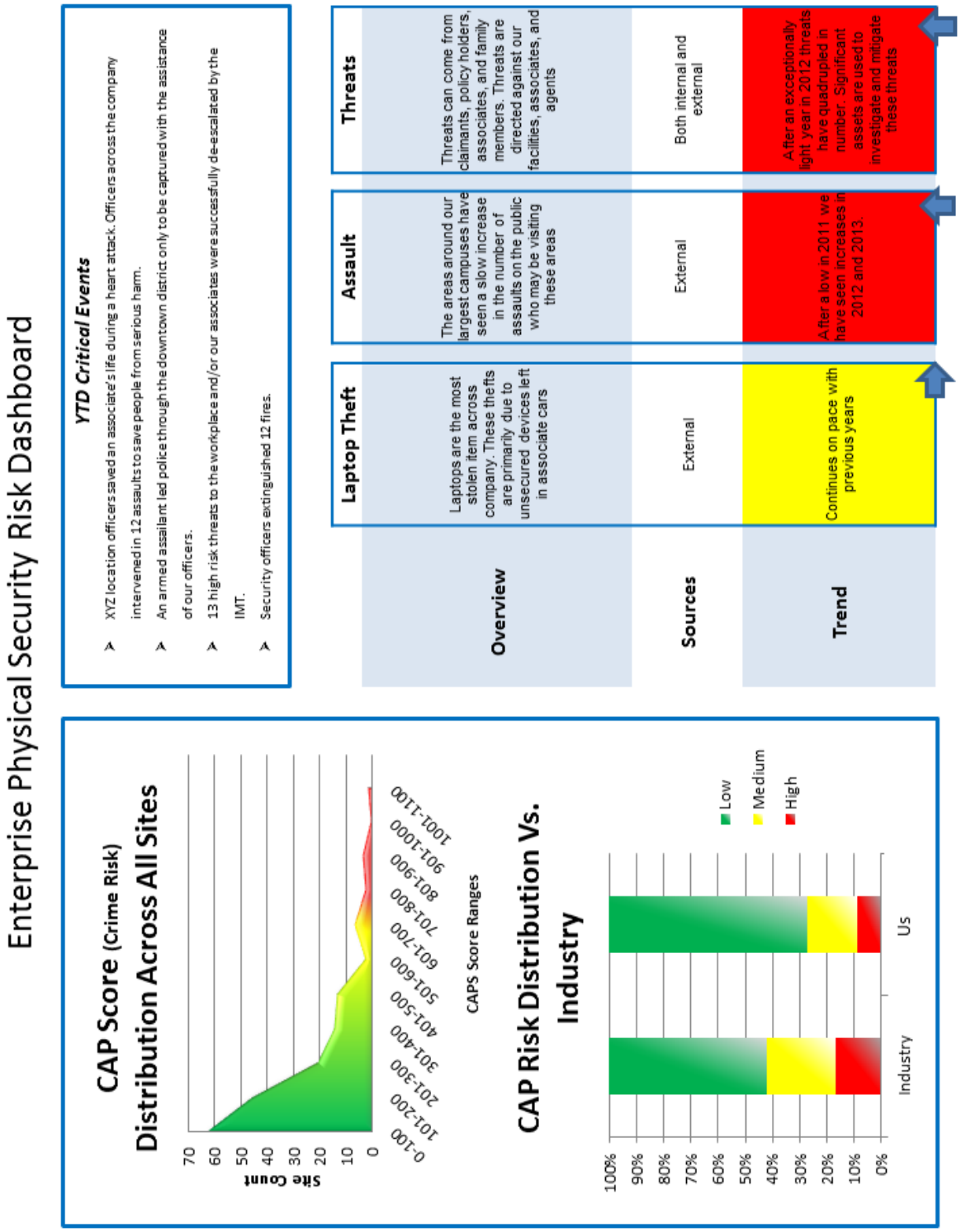
Most of the data is objective, and data collection is timely. The initial design of the data collection system for this metric required a significant amount of administrative time, but the ongoing cost is minimal.

This metric demonstrates a return on security investment in two ways. First, through the standardization that the policy calls for, the company can obtain long-term national contracts at favorable prices (e.g., alarm monitoring). Second, company surveys show that employees feel safe in corporate facilities and can work better when they feel safe. Thus, the metric, which increases site safety, measurably improves employee morale and productivity.

The metric helps senior management place facility site risk in perspective. Over time, it steers site selection toward safer areas. The metric also provides uniformity in specifying site security measures.

This metric puts security efforts into a language—the language of risk—that the insurance company's senior managers readily understand. The following graphic is an example of what the metric user presents to senior management:

Enterprise Physical Security Risk Dashboard



Expert reviewers (three rather than the usual two) and a member of the research team gave the metric the following scores, using the Security MET:

Metric 3	Researcher	Expert 1	Expert 2	Expert 3	
Criterion	**Score**	**Score**	**Score**	**Score**	**Average**
1. Reliability	4	3	4	5	4.00
2. Validity	4	3	4	5	4.00
3. Generalizability	3	4	4	5	4.00
Technical Total	**11**	**10**	**12**	**15**	**12.00**
4. Cost	3	5	5	3	4.00
5. Timeliness	5	5	5	5	5.00
6. Manipulation	4	4	4	5	4.25
Operational (Security) Total	**12**	**14**	**14**	**13**	**13.25**
7. Return on Security Investment	5	2	3	5	3.75
8. Organizational Relevance	5	5	5	5	5.00
9. Communication	5	4	4	5	4.50
Strategic (Corporate) Total	**15**	**11**	**12**	**15**	**13.25**
TOTAL ACROSS CRITERIA	**38**	**35**	**38**	**43**	**38.50**

The expert reviewers made the following observations:

> This is a useful tool for determining the risk associated with various sites and determining what security controls should be in place at each location. Ongoing review of CAP scores provides continuous evaluation. It might be beneficial to add other data sources to the metric, as well. The metric is straightforward, easy to maintain, and fairly easy to understand. Tying it to organizational policy increases the likelihood of consistent implementation of security measures.
>
> One could also attempt to measure or calculate the cost of security measures that would be needed to lower a site's risk score. Another metric could examine losses and incidents at a site both before and after implementation of countermeasures.

B. Personnel Security Clearance Processing Metric

At a defense contractor headquartered on the east coast of the United States, personnel security clearance processing is a vital step in the hiring process. The company hires about 2,500 new personnel per year, but because of the length and unpredictability of the clearance process, it generally was not possible to give candidates firm starting dates. Offering contingent start dates made the company lose good candidates to firms that offered firm starting dates. Moreover, each day of waiting for clearance processing was a day that the candidate could not be employed on, and billed to, a project.

3. Environmental Risk Metric

1. **Respondent title**

   Assistant Vice President, Corporate Security

2. **Organization's location, field/industry, number of employees, number of sites, annual revenue (or other measure of size)**

   Insurance company in Midwest U.S.; revenue approximately $18 billion; hundreds of owned and leased facilities throughout the United States.

3. **Description of metric (what are you measuring, and in general why?)**

   This metric is designed to serve the risk management needs of the corporation. We [corporate security] have not named the metric, but it could be called an environmental risk metric.

   Our company owns or leases hundreds of facilities across the United States. They include offices, data centers, retail storefronts, and claim centers. On a regular basis, corporate security collects a suite of data, assigns weights to various factors, and develops a numeric score that places each facility into a low, medium, or high category of risk. For each risk category, written policy specifies a collection of security measures that should be in place at the site. Exceptions can be granted, but the systematic approach results in uniformity and in efficiency in decision-making and security systems contracting. Most important, the metrics-based approach helps senior management understand the level of risk in site selection and make informed decisions on risk management. In addition, over time, the metrics have steered the corporation toward having a smaller percentage of its locations in high-risk sites.

   The formula for our ongoing risk assessment metric is as follows:

   CAP Index Score (local risk analysis) [CAP Index is a commercial provider of crime risk forecasting. CAP stands for Crimes Against Persons and Crimes Against Property.]

   The average national crime rating score through CAP is 100. CAP is valued as follows:

   1 – CAP score of 100 or lower.

   2 – CAP score of 101 to 200.

   3 – CAP score of 201 to 300.

   4 – CAP score of 301 to 400.

   5 – CAP score of 401 to 500.

   6 – CAP score of 501 to 600.

   Locations with a score of 601 or more will not be considered as a location for an office. Industry benchmark indicates that only 7% of financial services offices are located in areas with a score of 600 or more

Type of environment:

1 – Non-critical: storage, empty space, surplus equipment. Locations that, if rendered inoperable, would have little or no negative impact on business processes.

3 – Sensitive: administrative, claims, trial office, sales office or other public contact. Locations that, if rendered inoperable, could have their work transferred to another location with little impact to the business.

5 – Mission critical: IT/data center, call center, headquarters. Locations that, if rendered inoperable, would negatively impact the business for an extended period.

Sensitivity of the asset:

1 – Low: Nothing of irreplaceable value including non-identifying records, furniture, low value equipment, perishable supplies, surplus assets. Facility may not be identified/branded as a corporate asset.

3 – Medium: Valuable equipment, associates, personally identifying records. Facility is branded as a corporate asset.

5 - High: Critical information/data, leadership associates, board members, cash/cash equivalents, and critical infrastructure. Facility is identified as an integral part of the corporation, branded and well known in the community.

Occupancy type:

1 – Unoccupied space

2 – Mixed tenant space

3 – Sole tenant

The risk levels are defined by the following total scores from the values above:

Low-risk location = 4 to 9 points

Medium-risk location = 10 to 15 points

High-risk location = 16 to 19 points

Corporate policy defines the security measures required at each level of risk.

4. **How long has the metric been used at the organization?**

   12 years.

5. **How reliable is the data you collect for the metric? Please explain.**

   Most of the data is objective. The CAP Index score comes from an outside source. Defining the use of the site (storage, data center, etc.) is fairly straightforward. Site sensitivity depends on contents, which are listed in the policy. Occupancy type is straightforward. The data seems reliable.

6. **How do you ensure that the conclusions you draw from your metric are valid? Please explain.**

   Every quarter I present our conclusions to the corporate risk committee. We compare our loss and incident history to our policy. We follow the numbers over time. We are then able to compare our plan, and the site ratings, to reality.

7. **Would your metric be useful to other organizations? In other words, is it generalizable?**

   I believe so, with customization.

8. **What is the cost of developing and administering your metric? This includes monetary and non-monetary costs associated with metric development and administration, as well as any negative consequences associated with collecting the data or using the metric (for example, data collection takes a lot of staff time or offends employees).**

   In terms of non-monetary costs, the metric seems clean—no negative consequences. We pay $130 for a CAP Index score, per location. The initial design of our data collection system for this metric required a significant amount of administrative time. There is also the ongoing monitoring of incidents. However, the ongoing cost is minimal.

9. **Can the data for your metric be collected in a timely fashion—so it is relevant for decision-making?**

   Yes, it is timely. Much of the process is automated. We use a Lotus Notes database to compile the data. The data comes in constantly.

10. **Could people fake the metric data if they wanted to? Is there any incentive for them to do so?**

    People could conceivably fake the data, but that would mean lying about verifiable facts—a fairly serious move. We feel the data is good.

11. **Can your metric be used to demonstrate a return on security investment?**

    Yes, in two ways. First, through the standardization that the policy calls for, we can spend right, obtaining long-term national contracts at good prices (e.g., alarm monitoring). Second, in our company's associate engagement survey, employees have responded that they feel safe in our facilities, and that they can work better when they feel safe. Thus, our metric, which increases site safety, also improves employee morale and productivity as is measured by survey.

12. Is the metric aligned with your organization's goals, mission, objectives, assets, or risks? How?

One of my goals is to help the organization decide on its security risk appetite. I try to get senior leadership to pay attention and help decide how much risk to accept.

We had guidelines before. Now we have *policy*.

We're an insurance company. We like to keep people safe and minimize loss. This metric puts our security work into a language—risk—that senior management can understand.

13. Are your metric and metric results easy to explain to others—especially to senior management?

I create a PowerPoint with graphs and tables (included below). It is easy for senior management to understand.

14. How do you use the metric? What does it do for you? Does it guide your security decision-making?

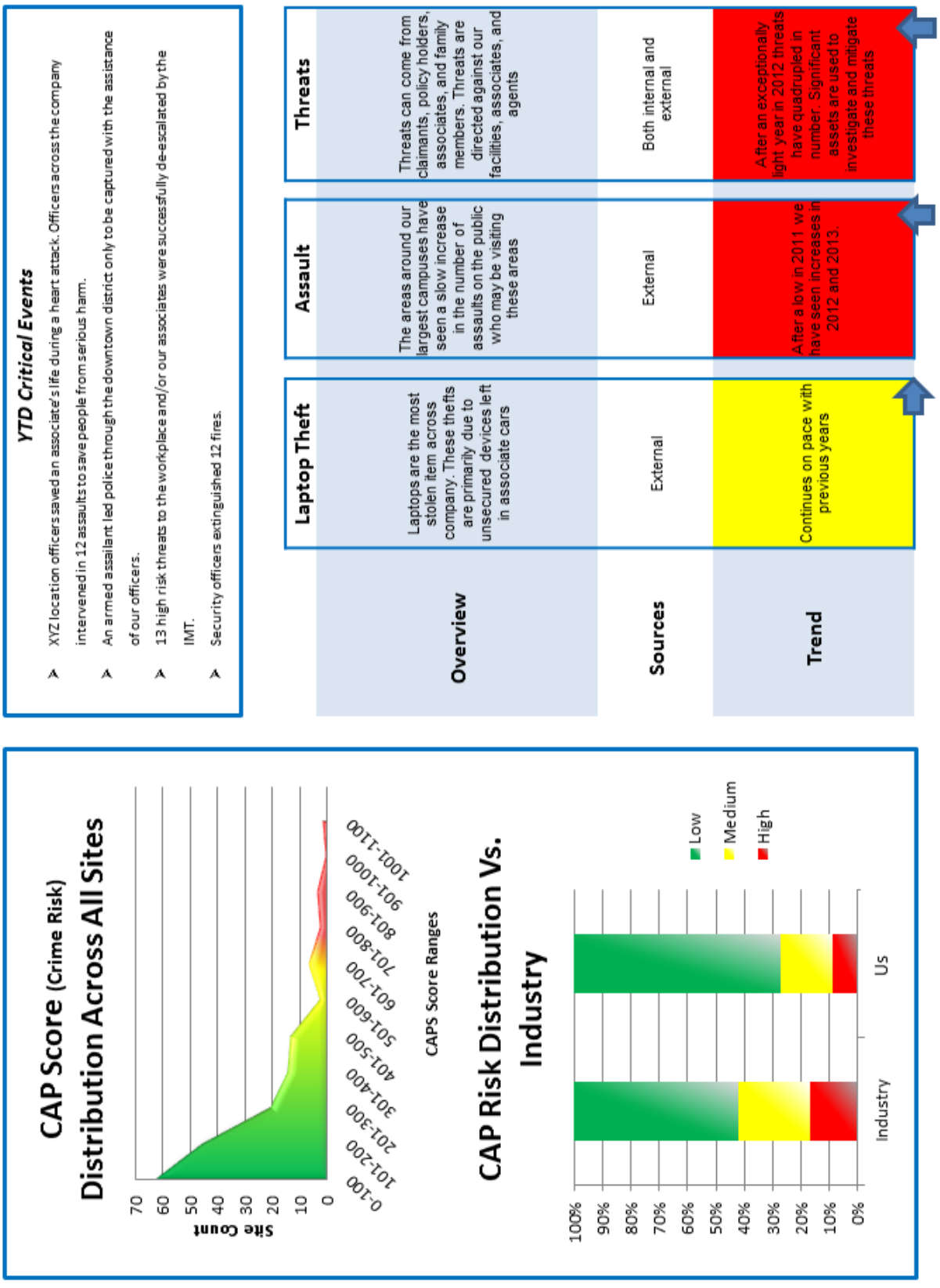
The metric helps senior management place facility site risk in perspective. Over time, it steers our site selection toward safer areas. The metric also gives us uniformity in specifying site security measures, provides economies of scale in contracting, and measurably adds to employee feelings of safety at work.

15. Can you share specifics—for example, specific measurements over time, specific security changes you made in response to the metric, and whether those changes had the desired effect?

Since we instituted the metric, security measures at headquarters have been accompanied by a roughly 50 percent decline in security incidents there.

Enterprise Physical Security Risk Dashboard

The following is an example of a graphic we would present to senior management:



Scoring and Comments from Reviewers

Based on the Security Metrics Evaluation Tool (Security MET)

Metric 3	Researcher	Expert 1	Expert 2	Expert 3	
Criterion	**Score**	**Score**	**Score**	**Score**	**Average**
1. Reliability	4	3	4	5	4.00
2. Validity	4	3	4	5	4.00
3. Generalizability	3	4	4	5	4.00
Technical Total	**11**	**10**	**12**	**15**	**12.00**
4. Cost	3	5	5	3	4.00
5. Timeliness	5	5	5	5	5.00
6. Manipulation	4	4	4	5	4.25
Operational (Security) Total	**12**	**14**	**14**	**13**	**13.25**
7. Return on Security Investment	5	2	3	5	3.75
8. Organizational Relevance	5	5	5	5	5.00
9. Communication	5	4	4	5	4.50
Strategic (Corporate) Total	**15**	**11**	**12**	**15**	**13.25**
TOTAL ACROSS CRITERIA	**38**	**35**	**38**	**43**	**38.50**

Expert comments:

This is a useful tool for determining the risk associated with various sites and determining what security controls should be in place at each location. Ongoing review of CAP scores provides continuous evaluation. It might be beneficial to add other data sources to the metric, as well. The metric is straightforward, easy to maintain, and fairly easy to understand. Tying it to organizational policy increases the likelihood of consistent implementation of security measures.