A Model to Quantify the Return On Information Assurance

Ron Greenfield and Dr. Charley Tichenor
Defense Security Cooperation Agency

Forecasting—and subsequently measuring—a program's financial return is an indicator of how well it supports its parent organization's strategic plan. This can help prioritize investments and help forecast and subsequently measure an individual's or team's job performance. This article presents a model to either forecast the financial Return on Information Assurance (ROIA) for Information Assurance (IA) countermeasure(s), or measure the financial impact of actual costs and the benefits of their use[1].

This article explains and demonstrates the structure of a model for forecasting, and subsequently measuring, the ROIA, or the ROIA model[2]. This includes IA initiatives such as firewalls, antispyware software, antivirus software, etc. Also, it can be used to determine the actual return of those countermeasures at the end of a given time period. Organizations are encouraged to either use this structure *as is* or modify it, and then populate it with their local variables[3].

Review of the Related Literature

Two important references apply to this research.

The first is the book "The Balanced Scorecard: Translating Strategy Into Action" [1], which measures Return on Investment using four categories:

1. Financial.
2. Customer satisfaction.
3. Improvement of internal processes.
4. Investment in learning and growth.

The currently formulated ROIA model only considers the financial category. This is not to downplay any other facet of IA, such as unintentional disclosure of information, loss of reputation, etc., which locally may be of equal or greater importance. This only means that there is room for future research to improve the ROIA model to address the Return on Investment of non-financial benefits.

The second reference is from Australia, specifically the New South Wales (NSW) Department of Commerce's "Return on Investment for Information Security" model [2]. The ROIA model is based on the NSW approach, although there are particular modifications. For example, Table 1 shows a modified version of the corresponding NSW table[4], and Table 2 is borrowed with little change although it is used somewhat differently here.

Theory

We define the term *return* as a measure of the degree to which a program is beneficial to the organization. Conceptually, it can be calculated as follows:

$$\frac{\text{\$ Benefits}}{\text{\$ Costs}}$$

For example, suppose a program costs $1,000, and brings in $1,500. The financial return could be then calculated as:

$$\frac{\text{\$1,500 gain}}{\text{\$1,000 cost}}$$

or, 50 percent. All other things being equal, the organization's balance sheet shows an increased bottom line of $500.

Using another example, suppose a program costs $1,000, but instead results in a cost avoidance of $1,500.

The financial return could be then calculated as:

$$\frac{\text{\$1,500 cost avoidance}}{\text{\$1,000 cost}}$$

or, 50 percent return. All other things being equal, the organization's balance sheet also shows an increased bottom line of $500.

The ROIA model generally views *return* in this second sense, as long as the organization's bottom line improves as measured using the U.S. Federal Accounting Standard Advisory Board's Generally Accepted Accounting Principles.

One IA goal is to either prevent or reduce future incidents of *successful* malicious attacks. Installing countermeasures can help achieve this goal. The ROIA model is currently based on how well the countermeasures reduce the *repair or replace* costs of forecasted future attacks. Countermeasures could include special software, such as antispyware software, security-related hardware, or IA training.

Therefore, we incorporate the following general concepts into the model:

- Current probabilities of successful attacks.
- Costs to repair or replace materiel as a result of successful attacks occurring before countermeasures are installed.
- Costs to repair or replace materiel as a result of successful attacks occurring after countermeasures are installed.
- Costs of countermeasures to prevent or reduce successful future attacks.
- Return on Investment and financial present values.

Table 1: *Probability of Vulnerability. Potential Number of Threats per Individual Computer per Year*

Likelihood	How Often per Individual Computer?	# Occurrences per 365-Day Year per Individual Computer. *At Least —*	Statistical —	
			Mean	Distribution
Negligible	Unlikely to occur	0	0.25	Poisson
Very Low	Between 12 and 24 months	0.5	1.42	Poisson
Low	Between 6-12 months	1	1.93	Poisson
Medium	Between 1-6 months	2	7.04	Poisson
High	Between 1 week and 1 month	12	32.00	Poisson
Very High	Between 1 day and one week	52	155.00	Poisson
Extreme	From 1 to 20 per day, or more	365	500.00	Poisson

More specifically:

- The **financial benefits** are defined here as the forecast repair or replace cost *avoidances* due to installation of a countermeasure. Successful attack incidents are reduced.
- The **financial costs** are defined here as the forecast of the costs to procure the *countermeasure*, paid now, plus *the cost of its annual maintenance* that will be paid in the future.

Therefore, the ROIA is modeled as the following ratio:

(Forecast repair or replace cost *before* countermeasures) – (Forecast repair or replace cost *after* countermeasures)
Cost of countermeasures

Also, the actual ROIA is modeled as the following:

(Actual repair or replace cost *before* countermeasures) – (Actual repair or replace cost *after* countermeasures)
Cost of countermeasures

Forecasting Countermeasure Benefits

Let's forecast the ROIA of a hypothetical system needing four countermeasures for four vulnerabilities. Start by asking, "What is the likelihood of a significant spyware attack happening to a single computer that would cause a repair or replacement during a given year?" (which is the first vulnerability). We demonstrate assuming a five-year lifespan and a four percent discount rate for present value calculations[5].

The ROIA model is built into an Excel spreadsheet, with the Crystal Ball Monte Carlo Simulation[6] software added-in. Refer to Table 1 (extracted from the Excel spreadsheet) for a set of further assumptions. As shown in the table, there are seven degrees of attack likelihood, and frequencies are defined. For this demonstration, we forecast that the malware attack has a *Low* chance: happening at least once per year (Occurrences column) but on average 1.93 times per year (Mean column).

Note Figure 1 as we discuss how to compute the 1.93. We think that such malware-successful attacks will arrive at an individual computer in the same random way that cars *arrive* at highway toll booths—a *Poisson* arrival pattern (see Table 1). Crystal Ball requires a rate parameter for the Poisson. This is entered as 1.5, which is halfway between the 1 in Table 1's column 3 for a *Low* and the 2 for the *Medium*. The selected range has a *Low* value of 1 because we defined a *Low* as happening at least once per year. In theory, it could happen infinitely many times, so *plus infinity* is the high value. Given these parameters, Crystal Ball computes the average of this Poisson distribution as 1.93.

After forecasting the average (expected) number of occurrences of successful malware attacks per year, the cost to repair or replace equipment affected by those attacks needs to be forecasted. Table 2 is used as a guideline for assessing the criticality of each attack instance.

With this as a guideline, we forecast the cost to repair or replace on an individual basis for each type of successful attack (see Figure 2). For this demonstration, we model the criticality of a successful malware attack to be *Significant* and model the best-case repair or replace cost situation as $20. The most likely case is $150, and the worst case is $400. This is a triangular distribution, with an average computed by Crystal Ball at $190.

Table 3 (see next page) recaps this. For vulnerability number 1, the Internet service asset has a vulnerability of significant spyware attacks. It has a *Low* likelihood of happening, but if it happens the criticality is considered *Significant*. This should occur about 1.93 times annually per computer in our system, at an average cost of $190 to

Criticality	Description
Insignificant	Will have almost no impact if the threat is realized.
Minor	Will have some minor effect on the asset value. Will not require any extra effort to repair or reconfigure the system.
Significant	Will result in some tangible harm, albeit only small and perhaps only noted by a few individuals or agencies. Will require some expenditure of resources to repair (e.g. *political embarrassment*).
Damaging	May cause damage to the reputation of system management, and/or notable loss of confidence in the system's resources or services. Will require expenditure of significant resources to repair.
Serious	May cause extended system outage, and/or loss of connected customers or business confidence. May result in the compromise of large amounts of government information or services.
Grave	May cause the system to be permanently closed, and/or be subsumed by another (secure) environment. May result in complete compromise of government agencies.

Table 2: *Criticality per Instance of Successful Attack*

Figure 1: *Poisson Distribution of Number of Malware Attacks per Year*

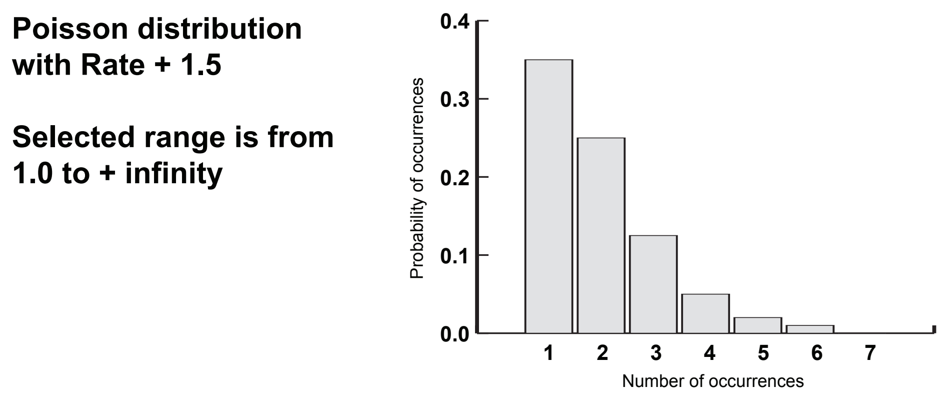
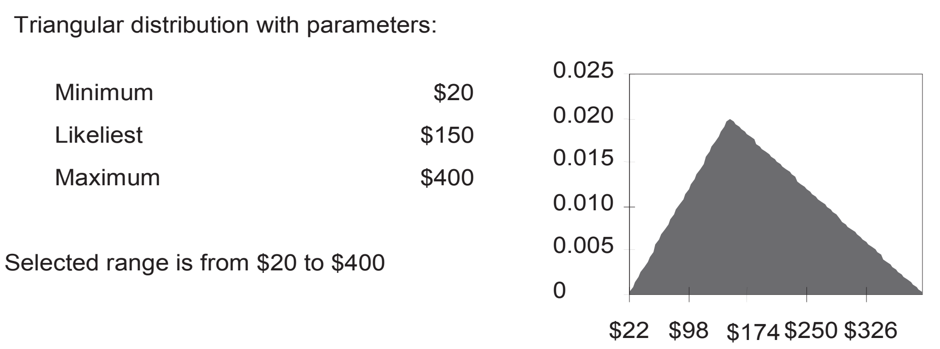


Figure 2: *Forecast Cost to Repair or Replace Due to a Successful Malware Attack*



No.	Asset	Vulnerability	"Before" Likelihood	Criticality	"Before" Number Occurrences per Year per Computer	Direct Cost per Incident	Number Computers	Agency Forecast Vulnerability Costs per Year "Before" Countermeasures Installed
1	Internet service	Significant spyware attack	Low	Significant	1.93	$190	100	$36,670
2	a	aaa	Medium	Insignificant	7.04	$37	100	$26,048
3	b	bbb	Low	Minor	1.93	$103	100	$19,879
4	c	ccc	Very Low	Damaging	1.42	$1,133	100	$160,886
.							**Total "Before" Vulnerability Costs ==>**	**$243,483**

Table 3: *Calculation of Expected Total "Before" Countermeasures' Installation Repair or Replace Cost*[7]

repair or replace the computer. For the 100-computer system, this amounts to an annual forecast average cost to repair or replace of $36,670.

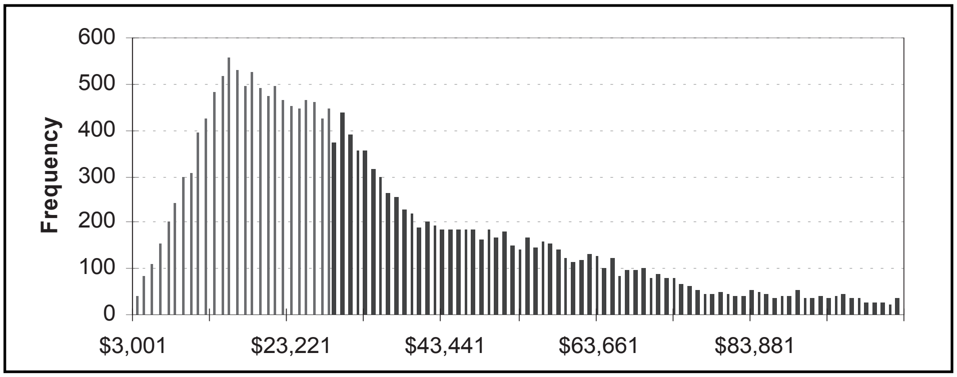
This calculation, however, is deterministic and does not account for the effect of the probability distributions. For example, although the average number of occurrences of successful attacks is 1.93, it could be 1 in a given year, or 2 in another year. Instead of multiplying the 1.93 *before* expected number of occurrences by the $190 direct cost per incident to repair or replace (and then by the 100 computers), we could—to get a better picture of what might actually happen—multiply the *before* occurrences distribution curve by the direct cost per incident distribution curve, and multiply that product by 100.

To forecast the expected cost *before* we buy the countermeasure, Crystal Ball selects a random number from the number of malware attacks probability distribution:

- This random number is converted into the *actual* number of times the threat occurs this year.
- Another random number is selected from the cost to repair or replace probability distribution, and this is converted into the *actual* repair or replace cost.
- These two values are multiplied together, and then multiplied by the number of computers (100).

This is repeated 20,000 times to produce a distribution curve for the annual cost to repair or replace (i.e., a Monte Carlo simulation run for 20,000 trials). Figure 3 shows a histogram plot of the outcomes.

Figure 3: *Forecast Vulnerability Costs for a Malware Attack "Before" Significant Spyware Countermeasure Installation*



The Monte Carlo simulation indicates that the possible annual cost to repair or replace all 100 computers ranges from about $3,000 to $84,000, with an average of about $28,782. This average value is where half of the area of the curve is to its left, and half is to its right, and that point can be read directly through Crystal Ball.

Assume that we now buy a countermeasure. To forecast the average cost to repair or replace *after* we buy the countermeasure, we multiply the cost to repair/replace by the number of times we expect it to occur and by 100 computers, as shown using Table 4.

For vulnerability number 1, the likelihood of a successful spyware attack *after* installation of the first countermeasure is modeled as *Very Low* but, if it happens, the criticality is considered *Significant*. This should occur 1.42 times annually per computer in a system, at an average cost of $190 to repair or replace the computer. For the 100-computer system, this amounts to an annual forecast average cost to repair or replace of $26,980.

As with the *before* costs, we determine the *after* costs distribution for this particular countermeasure using probabilistic methods. Figure 4 shows the *after* costs simulation results, and they are forecast to average $22,581 annually.

Each year's total deterministic benefit is calculated by subtracting its cost *after*

Table 4: *Calculation of Expected Total "After" Countermeasures' Installation Repair or Replace Cost*

No.	"After" Likelihood	Criticality	"After" Number Occurrences per Year per Computer	Direct Cost per Incident	Number Computers	Forecast Vulnerability Costs per Year "After" Countermeasures Installed
1	Very Low	Significant	1.42	$190	100	$26,980
2	Very Low	Insignificant	1.42	$37	100	$5,254
3	Negligible	Minor	0.25	$103	100	$2,575
4	Negligible	Damaging	0.25	$1,133	100	$28,325
					Total "After" Vulnerability Costs ==>	**$63,134**

countermeasures (Table 4, $63,134) from its total cost *before countermeasures* (Table 3, $243,483), or $180,349. Using a deterministic approach, we would multiply these totals by 5 (years) to obtain $901,745. However, using the probabilistic approach with the Monte Carlo simulation (see Figure 5), the average benefit (or cost avoidance) for those 5 years turns out to be $874,837.

Forecasting Countermeasure Costs

We now model the costs of the countermeasures. Here, there are four software countermeasure products installed. Each has an upfront purchase price cost, and each has annual maintenance. Refer to Table 5: Let's assume that these countermeasures will be *good* for five years each (this year and four subsequent years). The lower right corner cell is the sum of the five-year life span costs, or $98,200. This is known with certainty (by contract) and is not simulated.

Calculating the ROIA

The ROIA is now calculated by simulation. It is:

($ Benefits Curve [Figure 5])
(5 years of countermeasures costs)

The Figure 6 simulation (see next page) shows that it is possible that this program's ROIA could range from about -600 to about 1,900 percent. However, the *expected* ROIA in this *notional* example is 886 percent, and we are about 93 percent sure that the ROIA will be greater than 100 percent.

Net Present Value Calculation

The five-year ROIA forecast can be expressed in terms of *net present value*, which is an approach to comparing the worths of several alternate ways of allocating money.

For example, suppose that a person has $100 dollars. Let's look at two options on what they could do with that money:

- Option 1 might be to just put the money in their wallet; that allocation option has a *present value* of $100 because they could spend the $100 today.
- Option 2 might be to put the money in the bank, say, for one year at an interest rate of 4 percent; after one year, the investment would be worth $104. The money having a present value of $100 has an associated future value of $104.

Which option has the most (financial) worth to this person? A financial analyst will say that the first option represents $100 of spending power today. Also, although the second option has $104 of spending power next year, by reverse engineering, the investment that $104 also represents, in theory, is $100 of spending power today. So the financial analyst will say that both ways of allocating money have the same purchasing power today. They both have the same net present value.

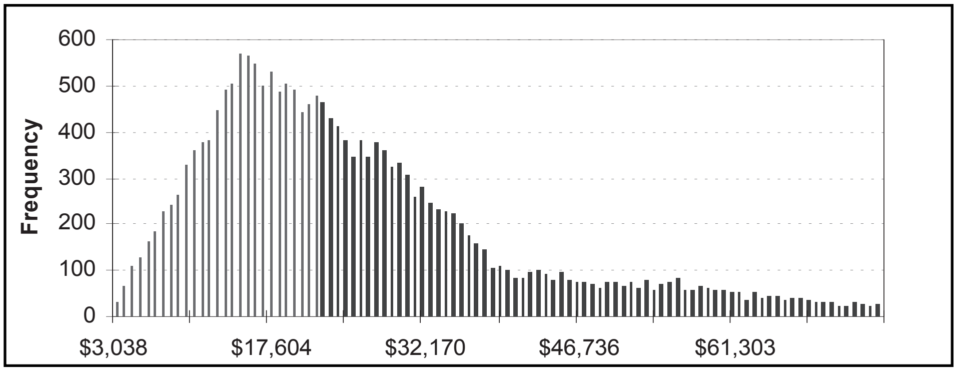


Figure 4: *Forecast Vulnerability Costs for a Malware Attack "After" Significant Spyware Countermeasure Installation*

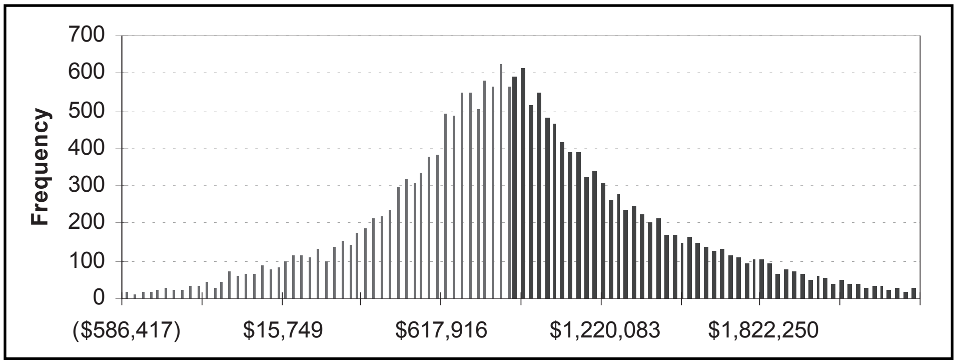


Figure 5: *Forecast Average Cost Avoidance for all Forecast Attacks "After" Countermeasures' Installations*

The ROIA model examines several financial allocations placed at different times in a five-year IA program. The theoretical purchasing power of those allocations today are calculated using net present value. That way the worth of these allocations can be forecast in advance. Or, after the five years are over and the actual results are known, then the actually realized net present value can be calculated.

For this simulation (shown in Figure 7, next page), the forecast net present value of this five-year IA program is $776,946.

Conclusions and Areas for Future Research

A quantitative forecast of an IA program's value is important to an organization. This model's basic paradigm is that at least a part of the financial ROIA can be quantitatively forecast as a measure of the effectiveness of countermeasures to possible system attacks. This can be formulated as the ratio of future cost avoidances due to those countermeasures to the cost of those countermeasures. This requires using probabilities of current and future successful attacks, costs of countermeasures to prevent or reduce future attacks, probable costs incurred as a result of successful attacks, and Monte Carlo simulations to obtain a distribution of forecast outcomes. The net present value of the IA

Table 5: *Actual Countermeasure Costs*

Counter Measures	Upfront Cost per Countermeasure	Recurring Annual Cost per Countermeasure Years 2 thru 5	Total Countermeasure Costs
Install anti-spyware software	$6,000	$600	$8,400
aaa	$20,000	$2,000	$28,000
bbb	$15,000	$1,500	$21,000
ccc	$10,000	$7,700	$40,800
	$51,000	**$11,800**	**$98,200**

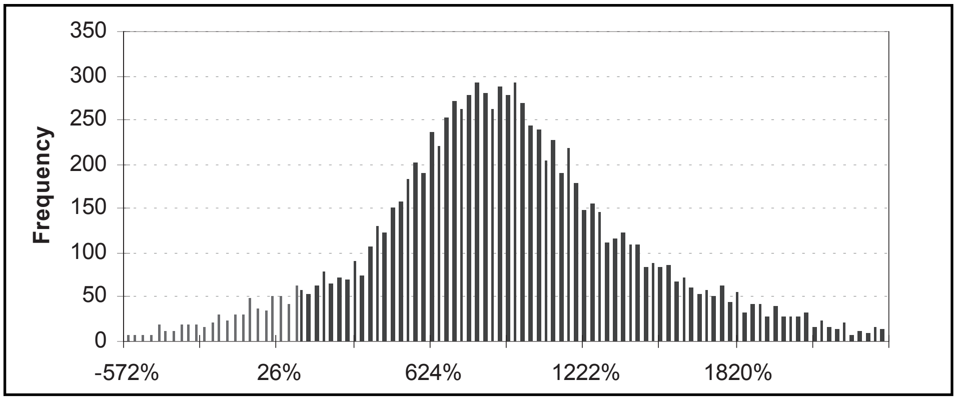


Figure 6: *Forecast Five-Year ROIA*

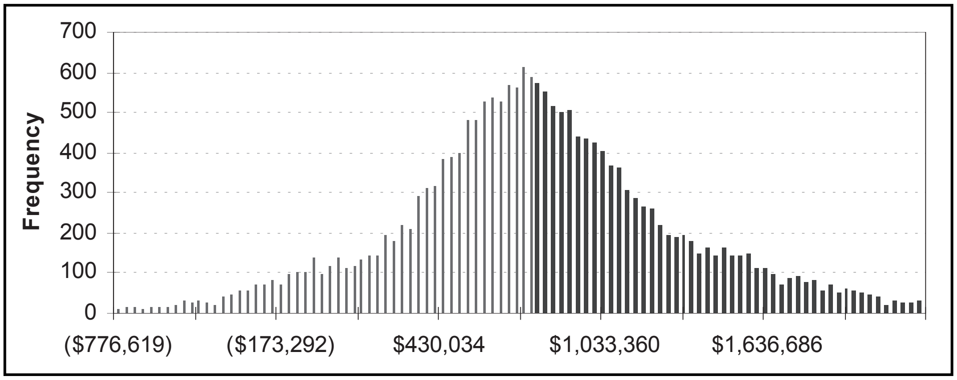


Figure 7: *Forecast Five-Year Net Present Value*

program can also be forecast.

It is also important to collect the data on actual cost avoidances as it arrives. The actuals can be used to build a knowledge base of cost/benefit information in improving future forecasting accuracy.

Future research might focus on ROIA in terms other than financial—such as the impact of compromised data. Which Balanced Scorecard perspective this might fall under, and how to quantify it, might be interesting and valued research.

Other research can include the impacts of risk mitigation. There is a standard deviation to the Monte Carlo simulation distribution curves, and the impact of new initiatives to the overall risk inherent in the IA countermeasures program could be forecast.◆

References

1. Kaplan, Robert S., and David P. Norton. The Balanced Scorecard: Translating Strategy into Action. Boston: Harvard Business School Press, 1996.
2. Government Chief Information Office, New South Wales (NSW) Department of Commerce, Australia. "ROSI Calculator." June 2004 <www.gcio.nsw.gov.au/library/guidelines/resolveuid/1549f99ec1ff7bcb8f7cb6cb8bceef8c>[8].

Notes

1. The views presented herein are solely those of the authors and do not represent the official opinions of the Defense Security Cooperation Agency.
2. This article is an abridgement of "A Model to Quantify the Return on Investment of Information Assurance" published in the *Defense Institute of Security Assistance Management (DISAM) Journal*, July 1, 2007. The authors thank the *DISAM Journal* for kind permission to provide this abridgement for CrossTalk.
3. The spreadsheet used here, and the associated PowerPoint presentation, is available from the authors. All numbers are notional.
4. For our purposes, we changed the definitions of frequencies of occurrence (see column 2), and eventually modeled the frequencies using a Monte Carlo simulation based on Poisson distribution. The NSW modeled them using the *max freq p.a.* values as expected values deterministically (i.e., as constants in their equations, not varying values in Monte Carlo simulation equations).
5. The five-year lifespan is used here as an arbitrary time frame for illustration purposes. Some DoD IA financial analyses use a six-year time frame. These (and all other assumptions) can easily be modified, as appropriate.
6. Crystal Ball software is a leading spreadsheet-based software suite for predictive modeling, forecasting, Monte Carlo simulation, and optimization. All figures are established utilizing Crystal Ball Predictive Modeling Software.
7. The "aaa," "bbb," and "ccc" values in Table 3 and Table 5 represent general vulnerabilities and general countermeasures, respectively.
8. Model developed by Stephen Wilson. This reference is used with his and the NSW office's permission.

About the Authors

Ron Greenfield is the information assurance manager, Defense Security Cooperation Agency, Office of the Secretary of Defense. He is certified as an information system security officer, information system security professional, information system security manager, and personnel security background investigator.

Defense Security Cooperation Agency
201 12th ST South STE 203
Arlington, VA 22202
Phone: (703) 604-6579
Fax: (703) 602-7836
E-mail: ronald.greenfield@dsca.mil

Charley Tichenor, Ph.D., serves as an information technology operations research analyst for the DoD, Defense Security Cooperation Agency. He has a bachelor's degree in business administration from Ohio State University, an MBA from the Virginia Polytechnic Institute and State University, and a doctorate in business from Berne University.

Defense Security Cooperation Agency
210 12th ST South STE 203
Arlington, VA 22202
Phone: (703) 901-3033
Fax: (703) 602-7836
E-mail: charles.tichenor@dsca.mil