Selling Security's Value Proposition

In the recent past, three things occurred at roughly the same time. I recorded an interview concerning a recent article in this space about advertising information security.[1] ISACA® issued a survey report on the state of privacy in 2023.[2] And some colleagues of mine published an article entitled, "ESG Is Dead—Long Live ESG."[3] This confluence of events kicked off some thoughts in my mind, which I would like to share.

> Privacy specifically and information security generally should always be considered as part of any organization's achievement of its mission.

Advertising Information Security

To recap the interview and the article it was based on, I had noticed that vendors of hardware, software and information technology services were advertising the security of their products on television. I wondered why businesses that implemented these products were not touting the ways that they secured information, especially that of their customers. My opinion is that these organizations were fearful that the goodwill that such ads might generate could be wiped out by a single cyberattack. In conclusion, I wrote that information security professionals "should aid their marketing departments in developing ad campaigns featuring what is being done to protect customers' information."[4]

Privacy and Profit

In the privacy report, there is an analysis of survey results on how boards of directors view privacy programs. The alternatives given were compliance-driven and ethics-driven. I was intrigued by the question not asked: There was no option for *profit-driven*.[5] I believe that directors of private-sector companies should always be considering profits, with no disrespect to compliance or ethics. Those organizations that are not driven to make money (e.g., the public sector, nongovernment organizations [NGOs]) should be *mission-driven*. The point is that privacy specifically and information security generally should always be considered as part of any organization's achievement of its mission.

Environmental, Social and Governance

ESG is a common acronym (at least in investment circles) for environmental, social and governance. The term implies that investments should be made with consideration of factors that go beyond financial returns. In some political circles, this is said to be "woke capitalism." In others, it is thought that investors should be doing good as well as making money. Just as I would never offer legal advice, I will not give investment advice. (Believe me, you do not want my investment advice.) But I will frame the argument in terms that are relevant to information security.

STEVEN J. ROSS | CISA, CDPSE, AFBCI, MBCP

Is executive principal of Risk Masters International LLC. He has been writing one of the *Journal*'s most popular columns since 1998. Ross was inducted into the ISACA® Hall of Fame in 2022. He can be reached at stross@riskmastersintl.com.

LOOKING FOR MORE?

- Read *Governance Roundup–What Are You Doing About Environmental, Social and Governance Factors in Your Enterprise? www.isaca.org/governance-roundup-esg*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

I believe that information security contributes both socially and in terms of governance. We humans cannot maintain meaningful social coherence without security overall. To the degree that our digitized world is fueled by information, much of it personal information, security provides the sinews that hold the body politic together. To those who argue against ESG, I would ask: Would you invest in a company that did not have sufficient security? Would you run a company that way?

As I see it, information security may or may not be tied directly to profits, but it definitely adds value to an enterprise: shareholder value in the case of publicly traded corporations; taxpayer value for the public sector. The problem is that we who specialize in the field have done a poor job of demonstrating that value. I suggest that we have been valuing and evaluating security based on the absence of breaches. In other words, we have put the burden of proof for information security into the hands of criminals. This is not an ideal marketing strategy. A much more positive approach is to project the value of security in terms of quality, reliability and value to the customer.

It is a truism—or at least it ought to be—that secure systems are better systems.

Security and Quality

Quality sells. This is true for everything from automobiles to zippers. It is a truism—or at least it ought to be—that secure systems are better systems. To achieve an acceptable level of security, designers must first reach a consensus on how secure their systems must be. Those that contribute to national defense require a higher level of security than those that, say, keep the bowling league scores. Software developers must work toward that consensus, while balancing factors including cost, time to market, customer demand, minimum customer acceptance and ease of use. Seeing security as a critical attribute[6] of systems leads to greater care in design, coding, testing and distribution. Hence my statement about the quality of secure systems.

It follows that the quality of security is, from a customer perspective, a leading indicator of overall quality. Sales representatives need not claim that their products are impervious to all threats. They need only demonstrate the features and functionality that contribute to security to aid in the sale, if not to close the deal, and to assist buyers in justifying the purchase to their management.

Security and Reliability

I have written before that downtime is "the most significant metric of contemporary cyberattacks."[7] Nearly every enterprise does some business on the Internet, if only to display its advertising. If its Internet presence is down, it is effectively closing shop until the site can be restored. Now multiply that impact one hundredfold if a cyberattacker should close down all its systems.

From a business perspective, the issue is not so much availability as reliability of the enterprise for its customers and, to a lesser degree, for its suppliers. As long as systems are secure and can be protected from going down, the private sector can continue to make money and the public sector to carry out its missions. And if the preventive measures fail, rapid recovery is the next best thing. Reliability is a business objective in a way that fending off the bad guys can never be, and it is one that carries value in the marketplace.

Value to the Customer

An enterprise's customers will never know about the security software, the access controls, the disaster recovery plan, the network configuration, or any of the myriad controls and protections in their supplier's systems. Nor are customers really interested in these things. Their interest is in having some reasonable assurance that the data they give to the enterprise will not be disclosed; that the money they have deposited will not be stolen; that the products they order will arrive on time; and that the transactions they entered today will still be there tomorrow, unchanged. This implicit contract is the basis for customer loyalty, more enduring than free samples. Any salesperson knows the importance of retaining satisfied customers. To the degree that security is a contributor to retention, it adds to the bottom line.

If security professionals do not state profit and mission achievement as *raisons d'etre* for information security, no one else will do it. These factors are more comprehensible to people not attuned to the daily grind of keeping information in the hands of those authorized to use it and out of everyone else's. It is our story, and we should tell it.

Endnotes

1 Ross, S.; S. Kazi, "Advertising Information Security," ISACA® Page to Podcast, 28 February 2023, *https://www.youtube.com/watch?v=3tEZ8dF8z4k*. ISACA, thinking that I have not subtracted enough from the sum of human knowledge with my bimonthly column, has of late been recording interviews about the articles with me on its podcast.

2 ISACA, *Privacy in Practice 2023*, USA, 2023, *https://www.isaca.org/resources/reports/privacy-in-practice-2023-report*

3 Johnson, K.; R. Funston; T. Reeves; "ESG Is Dead—Long Live ESG: Guidance for US Pension Fiduciaries," Funston Advisory Services, 2023, *https://www.funstonadv.com/in-the-news/esg-is-dead-long-live-esg-guidance-for-us-pension-fiduciaries*

4 Ross, S.; "Advertising Information Security," *ISACA® Journal* vol. 1 2023, *https://www.isaca.org/archives*

5 I have addressed this general topic before in this space: Ross, S.; "What Is the Value of Security?" *ISACA Journal*, vol. 2, 2011, *https://www.isaca.org/archives*. I came from a different starting point at that time.

6 Security by design, if you will allow my borrowing the term.

7 Ross, S.; "It's About (Down) Time," *ISACA Journal*, vol. 5, 2022, *https://www.isaca.org/archives*