Advertising Information Security

So, I am watching a sporting event on television and a former employer of mine runs an advertisement that says its devices will solve my cybersecurity problems. Later in the match, another former employer tells the world that its consultants can produce privacy for my business. A full page advertisement in my Sunday newspaper tells me that this organization's software can give me peace of mind that my data are safe.

What is going on here?!? Everywhere I look, it seems that someone is trying to sell me information security.

Information Security for the Mass Market

I have been a specialist in information security long enough to remember the times when we few, we happy few in InfoSec had to fight for any recognition at all. The struggle for budget, personnel, tools and seniority had to be fought endlessly, as did the battle against the bad guys trying to break into our employers' systems and data. So, for me at least, seeing information security sold to the general public leaves me in shock.

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.

I am concerned that people at large will come to believe that information security can be achieved simply by buying it.

I understand that advertising is a reflection of reality, not reality itself. I have long been told that if I only buy the right products, I will be healthier, wealthier, wiser and sexier. None have worked so far. I actually have greater confidence that some of the security products and services that I see advertised will work as promised. But I am concerned that people at large will come to believe that information security can be achieved simply by buying it. Yes, tools are important, but the security program that chooses and uses those tools is paramount.

There is something wondrous about advertising information security products to mass markets. It implies that the number of actual buyers of these products is great enough that it pays manufacturers and service companies to reach out to them through the general media. ISACA® take note: Our members are a large cohort of valued potential customers.

It is also pleasing that my friends and family who have long asked me, "What is it that you do exactly?" now are treated to an explanation that neither trivializes nor aggrandizes information security. These ads tell them what I and every other information security professional I know has been saying for years: Information security is good for business.

It Pays Not to Advertise

But there is something missing. I do not see advertisements for the banks, insurers,

manufacturers, educational institutions, governments or any other industry that buys security products stressing their own security. If we make the case, as I often have, that information security creates a competitive advantage, why are these organizations not claiming it? Are they just shy? Are their information security practices not thorough enough? Have they not spent enough on people and products?

I believe that many organizations are spending appropriately large amounts of money on information security.[1] (On the other hand, I do not believe any of the reported global outlays, which, with a brief search of the Internet, vary from US$23 billion[2] to US$40.8 billion[3] to US$140.12,[4] which is quite a spread.) So why am I not seeing ads that say, "Do business with us! Your data are secure with us!"?

I believe the reason is that they are afraid their entire marketing strategy can be upset in an afternoon by a successful cyberattack. A demonstrated lack of security could instantly become a competitive disadvantage. I realize how unfair this is. Not naming names, but I know of many top-flight organizations with excellent information security functions that have been victimized by cyberattacks and frauds. If the best are not safe, what can lesser institutions say or do?

This has long been a dilemma for those information security professionals who have tried over the years to demonstrate the effectiveness of their programs. The burden of proof rests with the criminals and terrorists. The best team in the league occasionally loses a game; they do not get relegated to the second division for that loss. But a single cyberattack can undermine the credibility of an entire information security program. No wonder marketing executives conclude that it pays not to advertise the strength of their information security.

Promoting Information Security

I propose that it is the responsibility of organizations' information security functions to capitalize on what they are doing to enhance the business' public image. They should aid their marketing departments in developing ad campaigns featuring what is being done to protect customers' information. In a bygone era, banks built large and imposing branches to imply their solidity; they called themselves trust companies. Insurance companies named themselves after mountains and large rocks. Manufacturers were proud to print pictures of giant factories on their labels. All of this was to say, "We are here to stay. We look after you and your assets. You can trust us."

Organizations and their information security functions can capitalize on this security literacy by explicitly demonstrating what they are doing to prevent theft or misuse of customers' information.

Perhaps it is time to rebrand information security and privacy as more than fancy technology and super sleuths. Customers and prospects can be told that the information security department is their friend looking out for their data. The chief information security officer (CISO) might be styled as the customer information protection executive (CIPE). Of course, the function will continue to protect all information as well as that of customers, but the public image would be altered.

Then an advertising campaign might be launched featuring the CISO/CIPE and the security staff. There would not be, must not be, any guarantees of secure information. Rather, the ads might explain what the individuals are doing to protect customers' interests. Note that the individuals would be featured, not the organization. The point is that there are people—not a faceless, impersonal institution—looking after you.

In large measure, because cyberattacks have been so well publicized, the general population is increasingly well-educated about issues such as cybersecurity, privacy and access control. Those TV spots during ballgames for security vendors have not hurt either. Organizations and their information security functions can capitalize on this security literacy by explicitly demonstrating what they are doing to prevent theft or misuse of customers' information.

I urge organizations to change the imagery of security and the way they use information security as a marketing tactic. Enough of locks, armaments and bulldogs as our symbols. Organizations should stress what they are doing to allow authorized customers, and only them, to access their information, rather than placing the focus on keeping the wrongdoers out. The avatar for information security should be the school crossing guard, not the burly cop.

LOOKING FOR MORE?

- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Ultimately, advertising for information security should convey that security is beneficial for the customer, more than a way of preventing bad things from happening.

Endnotes

1 For example, the chief executive officer (CEO) of one of the world's largest banks said in an interview that his organization spends more than US$1 *billion* every year on cybersecurity. Bursztysnsky, J.; "Bank of America Spends Over $1 billion per Year on Cybersecurity, CEO Brian Moynihan Says," CNBC, 21 June 2021, *https://www.cnbc.com/2021/06/14/bank-of-america-spends-over-1-billion-per-year-on-cybersecurity.html*

2 Smith, R.; "Global Cybersecurity Spend to Hit $23bn in 2022 – Report," *Insurance Business America*, 3 June 2022, *https://www.insurancebusinessmag.com/us/news/cyber/global-cybersecurity-spend-to-hit-23bn-in-2022-report-408361.aspx*

3 Sava, J. A.; "Spending on Cybersecurity Worldwide From 2017 to 2021 (COVID-19 Adjusted)," Statista, 16 February 2022, *https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/*

4 Research and Markets, *Global Cyber Security Market, By Type, By Solution, By Industry Vertical, By Services, and By Region—Forecast and Analysis 2022–2028*, Ireland, 2022, *https://www.researchandmarkets.com/reports/5597513/global-cyber-security-market-by-type*