Cyber Decisions Only Executives Can Make

"Cybersecurity is not simply a technical problem." I have heard and read this many times (and have said it a few times, as well). If the *Harvard Business Review*[1] and *Forbes* magazine[2] say so, it must be true. Right?

Well, maybe so. But in my experience, most organizations look to IT generally, and their information security professionals specifically, to prepare for cyberattacks, protect against their occurrence, detect them should they occur and respond accordingly. It is only when an attack disrupts normal business operations that businesspeople realize that they should have prepared their operations and planned for continuity without the systems and data on which they rely.

Cyber Recovery Plans

To be fair, many enterprises do have plans for recovery from cyberattacks, often seen as disaster recovery preparation more so than for business continuity. Most of the literature I have read on the subject addresses the restoration of the affected systems and data, with only tangential mention of how the business will carry on while that is happening. For example, the US National Institute of Standards and Technology (NIST) has issued guidance on recovery from cybersecurity events.[3] Its stated audience is

> *[C]hief information officers (CIOs), chief information security officers (CISOs), Information [Sharing and Analysis Organizations] [ISAOs], commercial security services providers, and authorizing officials for systems.*[4]

Business leaders are not included.

I propose that there are matters related to recovery from cyberattacks that are purely business related, taking as a given that IT will take appropriate action to eliminate incursions and restore data. These matters are fundamental to an organization's posture on cybersecurity, and they need to be considered and decided on to the extent possible without knowing the specifics of an attack that has not yet happened. I further propose that it is incumbent on information security professionals to frame these issues for their executives and obtain their prior resolution.

Categorizing Cyberattacks

Not all cyberattacks are the same. A data disclosure is not a wipeout of all personal computers and is not destruction of the central network. The effects of the two examples given are different, as are the potential methods for overcoming them. A manufacturer might be far more concerned about an attack that incapacitates its production lines, while a pension fund would see few things more threatening than wholesale disclosure of members' information. No two organizations are the same, and no two experience the same events as calamities. Only senior executives can draw the line between a disturbance and a crisis. The determination of where that line is drawn—and crossed—is best made when heads are cool.

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

Is executive principal of Risk Masters International LLC. Ross has been writing one of the *Journal's* most popular columns since 1998. He can be reached at stross@riskmastersintl.com.

It is not that manufacturers ignore privacy violations or financial managers are unafraid of downtime. Rather, the degree to which resources should be accorded to addressing various consequences is an executive rather than a technical decision.

Loss Tolerance

In a similar vein, only senior executives can determine how much pain an organization can absorb. There are so many ways that the pain can be manifested in a cyberattack: revenue, cash flow, customer service, brand and reputation, personnel welfare, and on and on. Information security professionals can conduct business impact analyses to inform executives, but they are in no position to say how much is too much.

Much flows from that determination. To oversimplify, let us presume that an organization would lose US$1 million in sales per day from a destructive attack and IT projects that it could recover from total destruction of its databases in 30 days. An expectation of up to US$30 million in losses enables a calculation as to whether to buy cyberinsurance, how much to pay for it and how much to budget for prevention (to reduce the chance that an attack might occur) vs. recoverability (to reduce the number of days of downtime).

Critical vs. Noncritical Functions

It is a commonplace that the greatest efforts should be applied to recover an organization's most critical functions. But which are the most critical and who is to decide? Surely, those systems that support an organization's core purpose are paramount. Manufacturers gotta manufacture; financiers gotta finance; governments gotta govern. Is the need to pay their people of the same importance? What about paying suppliers? Or investors? Who is to set the priorities? Certainly not the people in IT.

And then, what should be done about functions that are not considered critical in a systems-related crisis? Should nontransactional activities such as legal, marketing or strategic planning be told to go home and do the best they can with manual methods? That may, in fact, be the only viable strategy, but it is not a decision to be taken lightly. If executive management does deem this to be the prudent path, it behooves these "left-outs" to plan for fending for themselves, perhaps by eschewing enterprise systems and adopting Software as a Service (SaaS) applications. In that way, they can continue their activities if the central network is brought down.

The degree to which resources should be accorded to addressing various consequences is an executive rather than a technical decision.

Shutting Down Systems (or Not)

In some types of cyberattacks, the bad guys force the issue of whether to close down an application, a subnet or the entire IT environment. If the system cannot be accessed or if the data are destroyed, it is *ipso facto* shut down. Slightly subtler, if there is evidence that either the algorithms or the data are so manipulated that they lose any semblance of integrity, management could choose to continue using the affected systems but, in all likelihood, would not.

But should systems be halted if a data breach has resulted in a broad disclosure of information? Keeping in mind that the information has already left the data center, should the impact of an attack be compounded by cutting off the use of applications on which the business relies? As with so many things in life, it depends. Have all the data been stolen? How important are those data? Would continued disclosure harm the business or the data subjects?

These are all very difficult questions to answer, especially in the midst of recognizing that an organization's systems are under attack. It would be best to decide on policy, or at least the principles for making a decision, in advance. Policy is not the realm of technicians.

To Pay or Not to Pay

It is easy to say that no organization should pay a ransom to cybercriminals. So easy that the UK's National Cyber Security Centre does not "encourage, endorse, nor condone the payment of ransom demands."[5] The Canadian Centre for Cyber Security warns that "Paying the ransom does not guarantee access to your encrypted data or systems."[6] In France, paying off the attackers is considered tantamount to funding terrorists.[7] And the US government "strongly discourages all private companies and citizens from paying ransom or extortion demands."[8]

LOOKING FOR MORE?

- Read *Reporting Cyberrisk to the Board of Directors. www.isaca.org/reporting-cyberrisk-to-bod*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

The moral issues are clear, as are some of the practical reasons not to pay. But when a business's very survival is on the line—and that may be the case with a particularly effective ransomware attack—it may make sense to hold the corporate nose and send off some cryptocurrency. For commercial enterprises are effectively the only ones facing a financial impact from such attacks. This can only be a decision taken at the highest executive levels. The executives who might be involved should be giving thought to what their decision would be well before they need to make it.

Information security professionals should educate themselves on these and related issues and bring them before executive management. But they should not attempt to be the decision makers themselves. They have neither the perspective nor the responsibility to do so.

Endnotes

1. Hanspal, L.; "Cybersecurity Is Not (Just) a Tech Problem," *Harvard Business Review*, 6 January 2021, *https://hbr.org/2021/01/cybersecurity-is-not-just-a-tech-problem*
2. Campbell, N.; "Cyber Security Is A Business Risk, Not Just An IT Problem," *Forbes*,11 October 2017, *https://www.forbes.com/sites/edelmantechnology/2017/10/11/cyber-security-is-a-business-risk-not-just-an-it-problem/?sh=5ca7d1387832*
3. Bartok, M., *et al.*; "Guide for Cybersecurity Event Recovery," National Institute of Standards and Technology, (NIST) Special Publication (SP) 800-184, USA, December 2016, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf*. Yes, this is a US publication and applies specifically only to US government agencies. But, NIST has done more to provide an intellectual framework for cybersecurity than any other institution.
4. *Ibid*., p. 2.
5. National Cyber Security Centre, "Mitigating Malware and Ransomware Attacks," United Kingdom, 13 February 2020, *https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks#:~:text=Law%20enforcement%20do%20not%20encourage,computer%20will%20still%20be%20infected*
6. Canadian Centre for Cyber Security, *Ransomware Playbook*, Canada, 30 November 2021, *https://cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099*
7. Article 421-2-2 of the French Criminal Code as quoted in CMS Francis Lefebvre, "An Endemic Phenomenon With Exponential Growth" (English version), 29 April 2021, *https://cms.law/en/fra/news-information/ransomware-attack*
8. US Treasury Office of Foreign Assets Control (OFAC), as quoted in *The National Law Review*, "Ransom Demands: To Pay or Not to Pay?" 24 September 24, 2021, *https://www.natlawreview.com/article/ransom-demands-to-pay-or-not-to-pay#:~:text=The%20recent%20OFAC%20Advisory%20states,and%20foreign%20policy%20objectives%20of*

ONE IN TECH
An ISACA Foundation

Join ISACA's Foundation in building the current and future **Digital Trust workforce** by fostering a **diverse and inclusive** pipeline of professionals.

www.oneintech.org