Steven J. Ross, CISA, CISSP, 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.*

Stanley Baldwin's Bomber

Stanley Baldwin was a British politician who won numerous national elections in the 1920s and 1930s. He was also one of Britain's worst prime ministers, leading His Majesty's government through the Depression and the rise of fascism with inaction that amounted to catatonia. Winston Churchill referred to him as "no better than an epileptic corpse."[1] He is largely forgotten today, but is remembered (somewhat) for one quote. In the early 1930s, explaining why military action would be futile, he said, "The bomber will always get through."[2]

Now let us move forward more than 80 years to a conversation I had with the chief information officer (CIO) of a major law firm. He told me that there was no sense in building protections against cyberattacks because, "if the Freedonian Army wants my data, I can't stop them."[3] He was, in effect, uttering an updated version of Baldwin's evasion. But Baldwin was wrong. In World War II, some bombers, alas, got through, but not all. Stout-hearted airmen and fast fighter planes stopped many of them. The cost and difficulty of attack were raised to a point that proved unbearable for the aggressors. And people crawled into shelters to mitigate their risk when a bomber did manage to drop its load. The same counterarguments, in my opinion, apply to cyberattacks and even to cyberwar.

If—which I do not for a moment believe—but if it were true that cyberattackers can penetrate any system, steal any information and subvert any safeguard, then there are certain things prudent businesspeople would do. Let us accept that dismal assumption for the sake of discussion and explore a few ideas of what you should do if the unstoppable bombers are on their way.

GET YOUR FIGHTER PLANES READY

Every organization should make certain that it has intrusion detection systems (IDS) and intrusion prevention systems (IPS) located at every entry point into its network. Having said this, it is probably impossible, since entry points are now every personal computer and, increasingly, every mobile device. Therefore, traffic from all of these should be directed to secure gateways, with IDS/IPS there looking for bombers on the horizon.

And right behind them should be well-managed firewalls and virus filters. It is a sad fact that this should need to be pointed out this late into the war, but too many firewalls are lowered too often to allow seemingly benign traffic to pass through; even the vendors have admitted that virus filters can be beaten.[4] There is a new generation of firewalls[5] that simply provides a higher level of security. Sure, they cost money, but so does getting bombed, which we have presumed here to be inevitable.

TRAIN YOUR FIGHTER PILOTS

Just as in physical warfare, the best safeguards need people to make them work. It is essential that every organization have personnel who can implement controls to prevent and deter attacks, detect them when they occur, and recover from them if a bomber does get through. I have previously referred to this cadre of specialists as a CyberCERT.[6]

Repelling cyberattacks is not an innate skill, but people can be trained to do it. If you want to have enough airmen on your side when the bomber approaches, you cannot wait until then to start their training. You need to build your air force before the battle is fought.

MAKE COPIES OF IMPORTANT STUFF

In a war, if you think the Ministry will be bombed, you make copies of critical documents and store them somewhere else. Well, we are in a war with cyberattackers, declared or not. So it is important to have backup copies[7] of critical data.

This applies even more so to software. As I have mentioned in several articles,[8] a trusted image of software is the bedrock on which cyberrecovery must be built. Cyberattacks occur because programs are penetrated, although there are exceptions to this statement.[9] Therefore, just as with data, it is critical to have copies of

software that is known not to have been infected. This may necessitate saving many generations of copies, potentially back to software releases.

HARDEN YOUR TARGETS

At a recent conference, Dennis Wenk of Seagate stated that, in his opinion, downtime attributed to hardware and software that were beyond their end of life caused more damage than that caused by cyberattacks.[10] I cannot say whether I agree or not about the relative impact today, but it is evident that you cannot shoot down a bomber with a pop gun. It is imperative that applications and the platforms they run on be up to date. They need to have not only the latest security safeguards, but also be as free of flaws as possible.

To pick only one example, Microsoft has published a list of 91 significant security vulnerabilities in Windows 2003,[11] which was taken off support in 2010. I have personally seen production systems running on this operating system since that time. Running outdated software on antiquated equipment is akin to waving a bright banner at a cyberattacker that says, "Drop bombs here."

HIDE THE CROWN JEWELS

Keeping in mind that the Freedonian Army cannot be stopped in its never-ending quest to penetrate your systems, it only makes sense to make certain it cannot get to your most sensitive information. There are some files that, if disclosed, would cause significant and irreparable harm to your organization. Therefore, they should not be accessible remotely nor ever be copied to portable media, including laptop computers. Note: This approach may be considered extreme.

> "Minimize your risk as much as you can and prepare to recover when the attack occurs."

Alternatively, and more practically, all sensitive data should be encrypted—at rest, in transit and in use. In terms of cost and difficulty, this may actually be more onerous than the previously suggested, if unrealistic, approach, but it is more likely to be put into practice.

PREPARE FOR WAR

In summary, if you think that successful cyberattacks are inevitable, you should minimize your risk as much as you can and prepare to recover when the attack occurs. Come to think of it, that is a pretty good strategy even if you do not think the bomber will always get through.

If you think of cyberattacks as war, which it is in both the figurative and literal senses, make yourself ready to win it. Do not just accept defeat before the big battles begin.

ENDNOTES

1 Halle, Kay; *Irrepressible Churchill*, World Publishing Company, USA, 1966, p. 131

2 Hansard, Official Report, 10 November 1932, United Kingdom, col. 632, vol. 270, *http://hansard.millbanksystems.com/commons/1932/nov/10/international-affairs#column_632*

3 He actually referred to an army other than that of Freedonia, a small, imaginary country with an economy based largely on poultry, which considers all other nations to be sworn enemies.

4 See my previous column, "Barbarians at the Ramparts," *ISACA Journal*, vol. 3, 2013.

5 See the article by my colleague, Eric Beck, "How Zero-trust Network Security Can Enable Recovery From Cyberattacks," *ISACA Journal*, vol. 6, 2014.

6 *ISACA Journal*, vol. 5, 2014

7 Note that I said "backup copies" and not "replicated files." It is still important to have portable copies of data that have integrity (or at least as much integrity as usual) so that files can be restored to a known, trusted point. Replication provides a file that is current, but it does not preserve a trail of what it was, notably prior to being attacked.

8 See most recently my column, "Cyberrecovery Preparation," *ISACA Journal*, vol. 3, 2014.

9 Grimes, Roger A.; "Should You Worry About Memory-only Malware?" *InfoWorld*, 4 February 2014, *www.infoworld.com/article/2608848/security/should-you-worry-about-memory-only-malware-.html*. See also a comment made by Mr. Erik Taavila in regard to one of my previous articles, "CyberCERT," vol. 5, 2014, *www.isaca.org/Journal/archives/2014/Volume-5/Pages/CyberCERT.aspx#comments.*

10 Continuity Insights Management Conference, "Information Technology Risk: What You Need to Know," Scottsdale, Arizona, USA, 22-24 April 2105

11 I am not picking on Microsoft. It is only that Windows' security flaws are well documented. See *www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-107/cvssscoremin-5/cvssscoremax-5.99/Microsoft-Windows-2000.html.*