



- CIO/CTO Perspective
 - Policy and Regulation
 - Defense in Depth Security
 - Business Insights
 - Voice and Collaboration Solutions
 - IP Solutions
- Virtualization & On-Demand

Home » Blogs » lippard's blog

Availability is part of Security



Thu, 05/12/2011 - 07:24 | by [Jim Lippard](#)

"The only way to make a computer system 100% secure is to disconnect it from the Internet, shut off the power, and encase it in concrete, and bury it." If you've worked with people in the information security field, you've probably heard this or a similar exaggerated scenario of protecting information from threats by physically isolating it from the rest of the world.

Like 6

6

But this is a mistake, unless the objective is to create a time capsule for future archaeologists. The basic core elements of information security are described by the "CIA Triad": confidentiality, integrity, and availability. (There have been various recommendations for expanding [this core to include other elements](#), but there is little disagreement about these three.) The purpose of information security is to provide assurance for the correct functioning of a system with respect to security threats to these three elements. The information involved is kept confidential from those not authorized to have access to it, its integrity is protected against unauthorized changes, and it is made available to authorized users. While "encased in concrete and buried" may provide good controls for confidentiality, and to a lesser extent for integrity (though "bit rot" may quickly result in data loss), it provides no availability to authorized users. This means that such a scenario is ignoring the third element of security, and can't possibly provide "100% security" unless such limited availability is what is actually required.

The difficulty presented by "100% security" is like a philosophical concern about the impossibility of 100% certainty for knowledge—it's simply not often an actual requirement in the real world. What counts as "secure," like what counts as "knowledge," depends on context. Factors such as available resources, customer demands, the degree of willingness to accept risk, the consequences of a breach or loss, and the current threat landscape all provide relevant context.

And this points to yet another flaw in the scenario—it emphasizes preventive controls to the exclusion of detective and corrective controls. In the real world, breaches can and do happen, and it is important to be able to identify when they do and be able to recover from them. Security involves not just moats and locks to keep intruders out, but drawbridges and keys to let owners and authorized visitors in, and the people and processes that manage the technology. It involves building active capacities to detect and respond to changing threats, not just static obstacles.

The "encased in concrete and buried" scenario most likely receives initial plausibility because availability is not just a security concern. While loss of availability can result from a security threat—a denial of service attack, for example—it can also be produced by other causes which aren't classified as security threats, such as power outage, hardware failure, or even planned downtime for an upgrade. And availability is a primary concern of general IT staff, so security staff tend to focus on their unique contributions rather than what overlaps with the responsibilities of others. But this is generally a mistake—good security practice should be comprehensive, it should cover multiple functional areas, and it should serve to enable businesses to use information effectively. It's better to find the right balance of controls that promote all of the elements of security, rather than focus on confidentiality and integrity to the exclusion of availability.

Your Thoughts?

-Jim

Global Crossing can deliver security and networking in a single package. Our company continues a commitment to security that is unique to the industry. Since 1995, Global Crossing has managed the data network of the UK Government under the security accreditation, EAL 2. Now we have taken that further to forge a Network Security Agreement with the United States government. This agreement introduces broad sweeping controls to the access and management of our global IP network: affording you peace of mind about security. [Learn more](#)

Like

Follow Global Crossing



Languages

English

Search

Search input field with Search button

Connect on Facebook

Like Rory Goreé, Paula McElmeel and 1,809 others like this.



Cloud Services Suite

Click Again for Full Screen

User login

Username: *

Username input field

Password: *

Password input field

Log in button

[Log in using OpenID](#)

[Create new account](#)

Add New Comment

[Login](#)

[Request new password](#)



Type your comment here.

Showing 0 comments

Sort by oldest first

[M](#) [Subscribe by email](#) [S](#) [RSS](#)

Trackback URL

[Jim Lippard's blog](#)

Tags: [Defense in Depth Security](#) [availability](#) [CIA Triad](#) [information security](#) [IT](#) [resources](#)

Recent blog posts

- [Global Crossing Genesis Solutions International Events Part 2 of 2 - "Operationalizing the deal"](#)
- [Global Crossing Genesis Solutions International Events Part 1 of 2 "Winning the deal"](#)
- [IPv4 Addresses for Sale? Recap at IBC 2011 - Global Crossing Genesis Solutions Regional and global bandwidth expansion boom](#)
- [Tips to prevent voice communications systems fraud](#)
- [PSN Cost Savings in the UK Government Sector](#)
- [Advanced Cyber Attacks Require Sophisticated Technology](#)
- [Application management on Data Center critical environments](#)
- [Crowning glory for Global Crossing \(UK\) Telecommunications Limited](#)

[more](#)



Legal Disclaimer

Disclaimer: Opinions expressed here and in any corresponding comments are the personal opinions of the original authors, and do not necessarily reflect the views of Global Crossing. The content is provided for informational purposes only and is not meant to be an endorsement or representation by Global Crossing or any other party. This site is available to the public. No information you consider confidential should be posted to this site. By posting you agree to be solely responsible for the content of all information you contribute, link to, or otherwise upload to the Website and release Global Crossing from any liability related to your use of the Website.