



# No One is Immune


## Cybersecurity Myths and the Reality for Critical Infrastructure

The actual dimensions and intended consequences of today's cyberthreats are not understood clearly. News about cyberthreats has become so prevalent that suspicion of a cyberattack often is among the first considerations when we learn about damage or disruption to services in the public sector or when our critical infrastructures fail.

Myths and misconceptions abound about the reality of these threats, the organizations that are affected, and the level of preparedness appropriate to these entities. The consequences can be serious for our nation's critical infrastructure; companies that possess valuable intellectual property; and enterprises that store and process sensitive personal and private information. ICF International addresses the major myths below.

### MYTH#1


**We are a small player in the market. No one will target us.**



**REALITY:** Smaller companies may feel safe from cyberthreats. They assume that cybercriminals will target larger entities. Smaller infrastructure owners and operators may believe that malicious actors will not consider them large enough to be valuable targets. Whether or not smaller enterprises are the end target of a cyberattacker, they can serve as excellent proxies for cyberweapons testing and therefore are very much at risk. A cyberattack on a small utility—or bank, rail, or other public service—could serve as a useful proof of capabilities for the perpetrator, who also benefits from lower chances of detection and retribution. Perpetrators can learn how to conduct reconnaissance on networks they regard as characteristic of the networks they want to exploit or attack. They can study the effectiveness of their tools and tactics, then refine their capabilities on larger targets.

### MYTH#2


**We are big and have invested heavily already in cybersecurity. We are safe.**



**REALITY:** As some recent, widely publicized cases indicate, larger enterprises may not be as safe as they hope. Much work still needs to be done in the research and development community to understand the effects of sophisticated cyberexploits and attacks on increasingly complex infrastructures, including those that link traditional enterprise IT systems, mobile users, the cloud, and the "Internet of Things." Every device—be it a railway switch or an electrical power turbine—becomes a computer peripheral. Larger players, even those with sophisticated cybersecurity programs, may be especially attractive targets because the complexity of their networks outstrips the capabilities of their cybersecurity defenses.

### MYTH#3


**Our industrial control systems are air gapped and proprietary. They are safe from hackers.**



**REALITY:** In our interconnected world (the Internet of Things), the set of players with the means and motives to do harm is broadening. For companies with industrial control systems as part of their operations networks, knowing this threat is credible presents a window of opportunity. Control systems must be protected like every other IT system—with robust network monitoring, threat detection, and incident response—especially in machine-to-machine systems. Enterprise-wide cybersecurity needs to be extended to the industrial control and supervisory control and data acquisition systems on which our factories and infrastructures depend.

### MYTH#4


**We monitor monthly performance reports. We will know if we have a problem.**



**REALITY:** Last year's cyberattack on a German steel mill demonstrated the ability to reach and control a physical asset, not just gain access to information. We tend to worry more about data theft than data integrity, but a cyberattack on a physical asset demonstrates why monitoring is so critical and must be continuous. Spotting outlier data on a report after the fact is not good enough. In the real world, consequences happen too quickly.

### MYTH#5

**Our IT department takes care of all our cybersecurity issues.**



**REALITY:** If an enterprise suffers a cyberbreach or attack, every function feels the impact. In addition to concerns about sustaining operations, intellectual property may be put in jeopardy, customer personal and financial information may be compromised, and—for critical infrastructures—damage or disruption may pose a risk to life. Lack of preparation and failure to respond effectively can shake confidence in a breached enterprise. Financial and reputational damage can be severe, even unrecoverable. A whole-of-enterprise approach to cybersecurity preparation and response—with C-level and line-of-business leadership participation—affords regained business and mission operations. It also shows an upper hand regarding the enterprise's reputation through coordinated and consistent reporting to regulators, law enforcement, and other stakeholders.

Although perfect cybersecurity may be unobtainable, effective cybersecurity is within our reach. An enterprise can function confidently, and critical infrastructures can sustain operations despite rising cyberthreats. We only will gain that level of confidence, however, by being realistic regarding today's cybersecurity challenges.

To learn how ICF can help, visit [icfi.com/cybersecurity](https://icfi.com/cybersecurity)

ICF International (NASDAQ:ICFI) provides professional services and technology solutions that deliver beneficial impact in areas critical to the world's future. We partner with clients around the globe to help them define and achieve success.