Security Essentials

1. Build a Risk-Aware Culture
The idea is elementary. Every single person can infect the enterprise, whether it's from clicking a dubious attachment or failing to install a security patch on a smart phone. So the effort to create a secure enterprise must include everyone. Building a risk-aware culture involves setting out the risks and goals, and spreading the word about them. But the important change is cultural. Think of the knee-jerk reaction — the horror — that many experience if they see a parent yammering on a cell phone while a child runs into the street.

2. Manage Incidents and Respond
Say that two similar security incidents take place, one in Brazil, the other in Pittsburgh. They may be related. But without the security intelligence needed to link them, an important pattern — one that could indicate a potential incident — may go unnoticed. A company-wide effort to implement intelligent analytics and automated response capabilities is essential. Creating an automated and unified system will enable an enterprise to monitor its operations — and respond quickly.

3. Defend the Workplace
Cybercriminals are constantly probing for weaknesses. Each work station, laptop or smart phone provides a potential opening for malicious attacks. The settings on each device must not be left up to individuals or autonomous groups. They must all be subject to centralized management and enforcement. And the streams of data within an enterprise have to be classified, each one with its own risk profile and routed solely to its circle of users. Securing the work force means vanquishing chaos and replacing it with confidence.

4. Security by Design
Imagine if the auto companies manufactured their cars without seat belts or airbags, and then added them later, following scares or accidents. It would be both senseless and outrageously expensive. In much the same way, one of the biggest vulnerabilities in information systems — and wastes of money — comes from implementing services first, and then adding security on as an afterthought. The only solution is to build in security from beginning, and to carry out regular automated tests to track compliance. This also saves money. If it costs an extra $60 to build a security feature into an application, it may cost up to 100 times as much — $6,000 — to add it later.

5. Automate Security Hygiene
It happens all the time. People stick with old software programs because they know them, and they're comfortable. But managing updates on a hodgepodge of software can be next to impossible. Additionally, software companies sometimes stop making patches for old programs. Cyber criminals know this all too well. In a secure system, administrators can keep track of

every program that's running, can be confident that it's current, and can have a comprehensive system in place to install updates and patches as they're released

6. Control Network Access

Consider urban crime. Policing would be far easier if every vehicle in a city carried a unique radio tag and traveled only along a handful of thoroughfares, each of them lined with sensors. The same is true of data. Companies that channel registered data through monitored access points will have a far easier time spotting and isolating malware.

7. Security in the Cloud

Cloud computing promises enormous efficiencies. But it can come with some risk. If an enterprise is migrating certain IT services to a cloud computing, it will be in close quarters with lots of others — possibly including scam artists. In that sense, a cloud is like a hotel in which a certain percentage of the customers have bubonic plague. To thrive in this environment, guests must have the tools and procedures to isolate themselves from the others, and to monitor possible threats

8. Manage 3rd Party Compliance

Say a contractor needs access to the system. How do you make sure she has the right passwords? Leave them on a notepad? Send them on a text message? Such improvising has risk. An enterprise's culture of security must extend beyond company walls, and establish best practices among its contractors and suppliers. This is a similar process to the drive for quality control a generation ago. And the logic is the same: security, like excellence, should be infused in the entire ecosystem. The ruinous effects of carelessness in one company can convulse entire sectors of society.

9. Secure Data and Protect Privacy

Somewhere in the trove lie the company's critical jewels, perhaps its scientific and technical data, maybe some documents regarding possible mergers and acquisitions, or clients' non-public financial information. Each enterprise should carry out an inventory, with the critical data getting special treatment. Each priority item should be guarded, tracked, and encrypted as if the company's survival hinged on it. In some cases it may.

10. Manage Identities

Say a contractor gets hired full time. Six months pass and she gets a promotion. A year later, a competitor swoops in and hires her. How does the system treat that person over time? It must first give her limited access to data, then opening more doors before finally cutting her off. This is managing the identity life cycle. It's vital. Companies that mismanage it are operating in the dark and could be vulnerable to intrusions. This risk can be addressed by implementing meticulous systems to identify the people, manage their permissions, and revoke them as soon as they depart.