CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Climate Change: Implications for Information Technology and Security

Key Message: Climate change requires new strategies for dealing with traditional IT and information security risks.

Executive Summary

"US military strategists, CIA analysts, international agency officials and Nobel Prize winning economists concur with the consensus of the world's scientific community: the climate crisis is a planetary security issue, as well as a national security issue for each of the one hundred ninety two countries that belong to the United Nations. But the climate crisis is also, by extension, a corporate security issue as well as a cyber security issue" [Power 2008].

In this podcast, Richard Power, a distinguished fellow with Carnegie Mellon University's CyLab, discusses why the issues surrounding climate change call for business leaders' attention, driven by profitability, financial success, corporate social responsibility, risk management, and security. Richard provides a seven step strategy that CSOs and CISOs can promote within their organizations.

PART 1: RISKS AMPLIFIED BY CLIMATE CHANGE; AND OPPORTUNITIES

Climate Change Amplifies and Activates Specific Risks

- Regulatory risk: Organizations need to adapt to updated and new regulations. Some business leaders are seeking regulatory guidance to better define their responsibilities.
- Supply chain risk: Business leaders should not depend on getting everything they need from traditional sources. Supply chain regulatory mismatches may also come into play, given global supply chain partners.
- Product and technology risk: New issues may arise around the production and use of existing products and technologies.
- Litigation risk: New risks may arise comparable to those in other fields such as tobacco and asbestos.
- Financial risk: Climate change will financially impact consumers, the use of natural resources, and global trade, and will likely require new measures to safeguard the business.
- Reputational risk: The need (or lack thereof) to exhibit a high level of corporate social responsibility in this area can affect reputation, positively and negatively.

Risk Matrix Perspective

Climate change is at the top of the risk matrix, given its effect and impact on all other categories of risk.

Risks associated with, for example, failed nation states, disease and pandemic, terrorism, and environmental threats are all aggravated by climate change.

As a result, the 21st century risk matrix is quite different from that of the 20th century.

Traditional risks such as insider threat and online organized crime remain with the same issues, threats, and factors, but can be impacted by risks surrounding climate change.

Making the Business Case to Senior Leaders

Effective arguments vary depending on the background and awareness of the CIO, CFO, or CEO. There is no common denominator that unlocks this issue for everyone.

The most effective argument is profitability and the financial success of the organization.

Going green can save significant money and resources, and serves as a tremendous business opportunity.

PART 2: A CORPORATE CLIMATE CRISIS STRATEGY FOR IT AND SECURITY: POINTS 1-4

Point 1: Intelligence and Risk Analysis

Monitor business risks on global, national and regional scales as well as in your market sector.

Understand what is happening with

- the weather
- natural resources
- global supply chains
- the geopolitical scene
- global, national, and regional economic issues

Point 2: Understand Your Business's Carbon Footprint

Actually looking at the numbers is going to blow your mind.

It is important to know how you can reduce your carbon footprint and the benefits that come with reducing it.

If you don't do this now, you will likely be compelled to by regulation in the future. (See also Gunther 2008.)

Point 3: Go Green

Going green is particularly important in your IT environment. IT resources currently consume as much energy as the airline industry and are escalating exponentially.

Richard's October 2008 CSO online article discusses significant improvements made by IBM (reduced annual energy usage by 80% and total floor space by 85%).

Point 4: Business Continuity

Re-evaluate and revise business continuity, disaster recovery and crisis management plans and capabilities.

New criteria include planning for multiple, simultaneous events that occur in unpredictable ways. Adaptability and flexibility are critical for an effective response.

Events are going to occur more frequently, be more intense, last longer, and have larger impact.

PART 3: STRATEGY POINTS 5-7; AND THE ROLES OF CSOs/CISOs

Point 5: Awareness and Education

Develop climate change awareness and education programs for your workforce, offering guidance for going green in staff professional and personal lives.

Awareness and training programs are delivery systems for your workforce and can be quite effective.

The issue needs to be made personal so people truly understand how climate change affects their day-to-day life. This

is analogous to talking to people about home PC security, child safety, and online identity theft as part of security awareness programs.

Point 6: Mobility and Travel Security

While reducing travel may lessen your carbon footprint, it may not be the best solution.

Dealing with extreme events and workforce displacement requires thinking outside the box on how best to re-establish work environments anywhere, anytime.

Travel security becomes increasingly important when dealing with deteriorating climate conditions.

Point 7: Cyber Security

Climate change affects confidentiality, integrity, and availability – the three pillars of information security.

In addition to the obvious impacts on availability, climate change can create new vulnerabilities that affect integrity and confidentiality as organizations implement new approaches to computing.

Role of the CSO/CISO

The chief security officer is in an ideal position to raise awareness on this issue and drive it forward. The need for ROI arguments tends to fade as leaders become aware of the importance of addressing climate change.

Security is ultimately about protecting what you value.

Resources

Power, Richard. "A Corporate Security Strategy for Coping with the Climate Crisis." CSOonline.com, October 1, 2008.

The Global e-Sustainability Initiative

The Alliance for Climate Protection

Daoud, David. "Beyond Power: IT's Roadmap to Sustainable Computing." IDC, October 2008. (registration required)

Gunther, Marc. "Carbon finance comes of age." CNNMoney.com/Fortune Magazine, April 17, 2008.

CNN Money.com, Fortune Magazine. The Business of Green website.