CYSE 200T - Discussion Board Posts

DISCUSSION BOARD: Protecting Availability

As the CISO of a publicly traded company, ensuring the availability of our systems is critical for business continuity and protecting the interests of our shareholders. Availability means making sure that our systems, applications, and data are up and running when needed by our users, employees, and stakeholders. To protect this, I would put several safeguards in place. For starters, I would set up redundant infrastructure, meaning systems and servers across different geographical locations. With load balancing and failover in place, if one system fails, traffic would be directed to another working system, preventing any significant downtime due to localized issues, whether from technical failures or natural disasters. I would also implement DDoS protection to deal with the growing risk of these types of attacks, which can overwhelm servers and knock services offline. Using cloud-based DDoS mitigation services or appliances, we could monitor traffic and filter out malicious attempts before they affect our critical systems. Additionally, I would ensure that all critical data is backed up regularly, stored securely in offsite locations and the cloud. A well-tested disaster recovery plan would also be a priority, with clear guidelines for how fast we need to recover from disruptions and how much data we can afford to lose in the process. Regular patching of systems and software would be part of the strategy as well, addressing any vulnerabilities before they can be exploited. On top of that, a solid incident response plan would ensure that we can quickly identify and address any threats to system availability. Finally, limiting access to critical systems through role-based controls, multi-factor authentication, and strict permission policies would further protect us from potential disruptions caused by unauthorized access. By combining these steps, we can ensure that our systems stay up and running, which is vital for the health of the company and its reputation in the market.

DISCUSSION BOARD: Ethical Considerations of CRISPR Gene Editing

BioCybersecurity presents several ethical concerns, particularly regarding the misuse of genetic data. One major issue is the potential for malicious code to be inserted into DNA, infecting the systems that interpret genetic information. This could lead to privacy breaches, identity theft, or even biological weapon creation. Additionally, questions arise about the ownership and control of genetic data. Individuals must have clear consent about how their genetic information is used, as unauthorized access or manipulation could lead to exploitation or discrimination. The concept of "Hacking Humans" also raises concerns about human rights, as genetic manipulation or cyberattacks could cause irreversible harm. Ethical considerations must prioritize privacy, consent, and transparency to protect individuals' rights. Strict regulations are necessary to ensure the responsible use of genetic data, ensuring innovation in biosecurity does not come at the cost of personal freedoms or safety. BioCybersecurity should be developed with these ethical principles at the forefront

DISCUSSION BOARD: Opportunities for Workplace Deviance

Cyber technology has created numerous opportunities for workplace deviance by providing employees with new tools and platforms to engage in unethical or inappropriate behavior. One significant factor is the anonymity and privacy offered by the internet, which can encourage employees to engage in actions they might avoid in a face-to-face setting, such as cyberbullying, harassment, or accessing inappropriate content during work hours. Social media platforms also contribute to workplace deviance, as employees can easily share sensitive company information or make negative comments about their employers or colleagues, either intentionally or out of ignorance of privacy settings, leading to potential breaches of confidentiality or damage to the company's reputation. Additionally, cyber technology makes time theft easier to commit, with employees spending extended periods on personal websites, social media, or shopping during work hours without immediate detection. The misuse of company data is another risk, as employees may use digital tools to steal confidential information, manipulate records, or access sensitive financial data for personal gain. Cyber espionage and hacking are also facilitated by the availability of technology, with employees potentially using their access to company networks to steal intellectual property or sensitive data. Moreover, the rise of remote work has led to reduced supervision, making it harder for employers to monitor employee behavior, which increases the likelihood of deviant actions like working on side projects or misusing company resources. In this way, cyber technology has made various types of workplace deviance more accessible, and it is crucial for employers to implement policies and technological safeguards to prevent and detect such behaviors.

DISCUSSION BOARD: The "Short Arm" of Predictive Knowledge

Given Hans Jonas' concept of the "short arm" of predictive knowledge, our approach to developing cyber-policy and infrastructure should be guided by ethical foresight, humility, and a strong sense of responsibility. Jonas emphasizes that while our technological capabilities are growing rapidly, our ability to predict their long-term consequences remains limited. In the virtual world, this means embracing the fact that even the most sophisticated systems cannot anticipate every potential abuse, vulnerability, or unexpected consequence. Policy must therefore be grounded in a precautionary principle—designing protection from the start, making things reversible, and favoring security over speed. Jonas also calls for a higher moral responsibility in the face of such power, which in this case involves placing human rights, privacy, and equity at the top of cyber-policy. Secondly, since technological change is so unstable, we must establish institutions and governance processes that are adaptive, inclusive, and accountable—drawing on a diversity of perspectives and returning repeatedly to policy frameworks. Finally, Jonas invokes intergenerational ethics and challenges us to think about how decisions regarding cyber-infrastructure today will impact generations to come. Thus, our policies must not only address short-term demands but also be sustainable, secure, and able to adapt in the long term.

DISCUSSION BOARD: From Verbeek's writing (Mod 6, Reading 4) Designing the Public Sphere: Information Technologies and the Politics of Mediation

Governing the Ungovernable:
Regulation in a Networked, Intelligified World

BLUF: With the decline of centralized state power and the rise of intelligent networked objects, regulation must evolve. The Short Arm of Predictive Knowledge reminds us that flexible embedded governance is the only sustainable path forward.

Why Traditional Regulation No Longer Fits

Verbeek (2015) shows how doors, mirrors, and cars now act intelligently and persuasively, far beyond the oversight of slow-moving governments. [6] This shift demands that markets and individuals share regulatory responsibility through decentralized mechanisms.

Embedding Ethics into Smart Technologies

When technologies shape behavior like smart mirrors offering lifestyle advice, regulation must be designed into the system itself (Verbeek, 2015). [7] Following The Short Arm of Predictive Knowledge, this anticipatory approach accepts we cannot foresee every outcome, but we can prepare systems to adapt.

Networking Responsibility in Real Time

Additionally, static rules can't keep up with dynamic connected technologies. [5] Instead, we need responsive systems of shared accountability among users, firms, and platforms to evolve with emerging risks.

Conclusion

The more intelligent and interconnected our world becomes, the less we can rely on centralized control. Embracing predictive humility means designing systems that regulate themselves, adapt in real time, and distribute responsibility across networks