I. The Internet of Things (IoT)

By the time you count 8 seconds or read the first section of this article, 150 new devices have been connected to the IoT. That means 61,500 per hour; 1,500,000 per day. Currently 7.4 billion devices are connected to the IoT, more than humans on the planet. By 2020, estimates of connected devices range from 26 billion to 75 billion.¹

The modern student and faculty are inextricably and innocently connected to the IoT. Their behavior will only exponentially increase the security threat to the educational institution.

II. Aliens Invade New Mexico

On May 15, 2017, the Albuquerque Journal reported a computer server breach at the University of New Mexico foundation had caused the University to notify 23,000 people of the incident. Not just “any people”, but donors, annuitants, foundation employees and vendors.² A memorandum sent to trustees of the foundation almost one month later states that an “unauthorized individual” had gained unauthorized access to a file server that contained contact information, donation amounts, check routing numbers, social security numbers and birth dates for 22,000+ donors as well as over 750 employees, vendors and annuitants of the University of New Mexico.³

³ Id.
The University did announce that its general data base of over 300,000 UNM alumni and donors had not been accessed. The almost 30 day lag between discovery and notification was reported as necessary to determine the breadth of the breach, to secure the system and to determine what and whose information might have been affected. A spokeswoman, Jennifer Kemp, offered that numerous legal and moral requirements created the lag between discovery and written notification of the breach.

III. Higher Education at a Crossroads: The Issues

- Cloud Security: Higher education is investing in modern infrastructure for interconnectivity, flexibility and ease of administration. All data in transit should be considered as potentially lethal.
- Performance: As schools consolidate their data centers, security must be flexible enough to meet the demands of swiftly changing virtualized environments and demand for network bandwidths.
- Valuable Data: Before New Mexico, higher education institutions have been prime targets for cyber criminals seeking monetization from theft of research, intellectual property, payment data, and student and faculty information. New Mexico provides the wake-up call that universities are also the repository of an incredible wealth of Personal Identity Information (PII) of some of the greatest wealth in the United States – their loyal donors.
- Appropriate Access for All: with students, visitors, faculty, administration, vendors and research partners all

4 Id.
5 Id.
6 The various federal and state notification laws (minimum of 47 possible notices) are clear. The application of morality to this established process is well beyond the scope of this author’s cyber-legal practice.
clamoring for universal access to a network, a proper balance must be struck between access and security – a daunting challenge.

- **The Overwhelming Challenge of the IoT:** The universe of access ranges from student smart phones to security cameras – ALL provide potential access to the network that is growing exponentially.
- **Distributed Environments:** Having a centralized security protocol for a population ever on the move and sometimes never present due to an increase in online education becomes the challenge of the rest for this decade.

### IV. Lessons Learned: A Universal Approach:

To date, the Target federal court published decision\(^7\) has offered agnostic invaluable advice for modern cyber security. In a case in which negligence was easily determined and damages of hundreds of millions of dollars have been awarded, the modern higher educational institution can ill afford to market its progressiveness while maintaining ignorance to the clear lessons at hand.

**A. Understanding the Parties and Information at Risk**

1. **The Students:** Our next generation of the best and brightest has PII that must be protected. Lest one believe that this group can be kicked down the road, the decision with the Vermont Attorney General and the University of Auburn should serve as sufficient warning with a settlement by Auburn University recognizing adherence to Vermont’s breach

\(^7\) In re: Target Corporation Customer Data Security Breach Litig., 66 F.Supp. 3d 1154 (D. Minn Dec 18, 2014 (No. 14-2522)); See also, Avoiding the Bullseye: Lessons Learned From The Target Litigation, by David Furr, published by the American Bar Association.
notification law or liquidated penalties up to $10,000 per violation.\footnote{Per violation presumably means per student. The Auburn action brought by the Vermont Attorney General arose from a discovered security vulnerability in a file server used by its College of Business on or about November 20, 2013. On February 4, 2014, the University determined that student PII of two (2) Vermont residents was present on a general file server, including social security numbers. Because the Vermont Attorney General was not notified for 119 days after the exposed vulnerability, the State Attorney General filed an action alleging the University failed to act in the most expedient time possible with no reasonable excuse. \textit{Cybersecurity 2015: Managing the Risk}, Practicing Law Institute, p. 169.} No actual breach has ever been alleged.

2. **The Faculty:** The PII of our faculty who are performing some of the most advanced research in the world can be easily exposed by a breach. The OPM breach should serve as dire warning to what exposure of critical PII can create with the advanced criminal mentality.\footnote{Estimates of 50 years of data theft from the U.S. government of critical PII and PHI that become critical for espionage have widely circulated.}

3. **Research and Grants:** The raison d’être of many of our institutions is the ideal pilferage for many nation-states seeking easy access to the development of our next generation of intellectual property. Leakage because of lack of basic cyber security extends far beyond the boundaries of ordinary negligence in this author’s opinion. Our own government’s lack of cyber security has led to extraordinary financial and defense losses with the recent announcements from both the SEC and Department of Defense.

4. **The Alumni:** Forget everything above, the heart and soul of the endowments of our greatest educational institutions rest with the charitable gifts provided by the wealthiest individuals and corporations in the United States. To accept these gifts, many of which have been created by a lifetime of work, in an unprotected manner is grossly negligent, if not
worse, in this author’s opinion. The University of New Mexico has served as a critical wake up call to every president, chancellor and the board of trustees of our educational institutions.

B. The Basic Solutions

1. Segmenting the Crown Jewels: Whatever percentages of enterprise risk you assign to the parties above, any basic cyber security protocol starts with segmentation of the network. The basic premise of segmentation is to isolate sensitive and critical data from the general network, using the concept of zero trust to allow content to be accessed only by a limited and identifiable set of users, through a well-defined set of applications, blocking everything else. Prevention of unfiltered ingress or data exfiltration is critical.

2. Multifactor Authentification and Encryption: Creating protected zones with specific and authorized entry is necessary in the modern security environment. These, along with segmentation, are the two pillars of modern cyber security.

3. Next Generation Firewalls – Utilizing a Platform Approach: With the migration and inevitableness of the cloud, IoT, online course delivery and virtualization, the institution must seek real time visibility and cohesive security for its cloud, network, end point devices and content. Only a platform based model can deliver:

- Next generation security capabilities – including firewall, IPS, decryption, unknown threat detection,
networking antivirus and URL filtering that work together to deliver application, user and content visibility and control, along with protection against network-based cyber threats.

- Threat intelligence that correlates, synthesizes and analyzes evolving threats and related metadata gathered from global platform deployments.

- Advanced endpoint protection that stops zero day exploits and modern malware on devices from network servers to remote laptops.

With the adoption of nextgen platform-based technology, the institution can:

- Gain granular visibility into network usage.
- Improve security posture with virtual network segmentation.
- Automatically prevent attacks and known threats from impacting students, faculty, alumni/donors, networks and research and data.
- Protect school-owned devices.
- Enable safe and secure remote access.
- Secure cloud use and SaaS applications.

**Conclusion:** Our higher education institutions have been both the bastions of academic freedom and our best resource for molding and defining the next generation of citizens and leaders of our nation as well as for research that will continue to define our role in the world. Supporting this fundamental premise and vision with an
underlying security posture that protects our most valuable data and people with layers of defense that respect confidentiality, integrity and availability is the basic challenge and responsibility of our institutions. Ignorance in light of the University of New Mexico incident is a shot across the bow that cannot be legally or morally ignored. While larger institutions can employ and manage the critical technologies discussed in this paper, smaller institutions can now rely on managed services from a security partner to provide “best in class” technology and resources required to protect and monitor their most valuable assets at very reasonable costs. If no other lesson has been learned from the University of New Mexico, a president having to send personal breach notices to the University’s 22,000 top donors that “unknown aliens have invaded” should strike fear into the heart and soul of every institution.

David M. Furr
dfurr@gastonlegal.com
704-790-6013