Background

Universities and colleges around the world are facing new and rapidly advancing forms of cyber-attacks, resulting in millions of dollars in remediation costs and reputational damage at elite schools. Since mid-2013, US universities have disclosed major security breaches at a rate of about one per month. It is reasonable to assume that more breaches occur which are not disclosed.

In recent years, the Internet threat landscape—the sum total of attackers, their methods, and objectives—has evolved with startling speed and ferocity. Today’s attackers are well organized, heavily resourced, and goal driven. Cornell is increasingly at risk due to this new generation of cyber-threat because it is:

- known to have valuable data, due to its stature as a preeminent research university with global reach and affiliations;
- fair game, without exception to the broader reality of sophisticated threats;
- a productive community with exponential growth in data and IT systems—more to manage means more at risk; and
- subject to a growing regulatory landscape in response to large incidents.

Like most of our peers, Cornell has historically emphasized end-user workstation protection, speedy incident response, and end-user awareness programs as forming the foundation for effective IT security practices. These measures are declining in effectiveness.

We need a new approach—to balance mission with risk.

Part of the challenge is to match not only the ingenuity of the attackers, but even more so the speed at which they are increasing in sophistication, persistence, and detection-avoidance. As would be expected, it is difficult for universities to combat adversaries who continually and rapidly change their tactics and technologies.

This report contains a summary of issues arising from the changing threat landscape, a brief update on noteworthy progress, and specific actions that must be taken to protect Cornell’s digital and financial assets, and its reputation.

The following recommendations are based on a simple premise: to balance mission with risk. For the benefit of the university community, IT security measures must continue to maintain a reasonable level of open scholarly access while also managing and mitigating risk in a rapidly changing digital world.

Issues Arising from the Changing Threat Landscape

1. **Resource constraints.** A small number of staff have been added to the IT Security Office (ITSO) while personnel levels across IT have declined. However, investment in security technology and standardizing business processes has lagged. The Ithaca campus spends less than 2% of overall IT monies on IT security. *This is the lowest among the Ivies and half the minimum IT security investment of a comparably sized corporation.*

2. **IT security policy.** Cornell has one of the most comprehensive collections of IT policies in higher education. The safeguards outlined in the campus security policy are effective only when applied consistently. Even so, modernization is necessary to stay abreast of the
changing threat landscape. Three challenges arise with regard to the inconsistent application of IT security policy:

a. **Variation in business practices.** The decentralized nature of the university means that operating units—at the level of colleges, schools, or departments—are responsible for ensuring local staff members comply with policy. Further, the ITSO’s core security program is dependent on a small number of non-CIT employees for whom security is an added job function. *History suggests a lack of uniformity in local business practices leads to inconsistent application of IT policy, thereby increasing risk to the entire institution.*

b. **Lack of built-in security for web systems and infrastructure.** Ensuring web-based applications are secure has proven problematic, especially when web development is distributed across the colleges and units. Measures such as best-practice coding, testing standards, vulnerability scanning, and penetration testing are irregularly applied. The proliferation of internally developed web applications, which have not been subject to appropriate security controls, is a significant risk. *Absence of these measures leaves university data and IT systems highly vulnerable.*

c. **Within policy and across the university, an overall higher baseline set of standards and safeguards is necessary to meet the challenges of the current threat landscape.** Policy needs to address the use of encryption, enhanced authentication systems, embedded systems, web application development practices, and other areas key to a defense that effectively balances mission with risk.

3. **Research data.** The university’s intellectual property and research data has not yet achieved parity with administrative data in terms of security safeguards, awareness, and incident response processes. A set of standards and safeguards was developed in 2014 but awareness and compliance across the university remains limited. *Prudent policy safeguards are needed to better protect both intellectual property and research data.*

4. **CIT practices.** The level and consistency of security safeguards also varies across CIT, with some areas following exemplary practices and others lagging. Technical safeguards in CIT should uniformly exemplify best practices as informed by the contemporary threat landscape and the optimal balance between fulfilling Cornell’s mission and managing risk. To realize this security goal, greater investment is required. *Technical safeguards must be built in to all CIT products and services.*

**Noteworthy Progress**

1. Cornell was one of the first universities to embark on a comprehensive risk assessment of its critical campus infrastructure (power generation, cooling, potable water, SCADA, etc.). That assessment is nearing completion and has uncovered laudably few risks in those environments.

2. Cornell has led the way in its approach to cloud vendors and IT outsourcing, including security assessments, contract language, and other measures that reduce risks to business continuity and data loss.

3. In 2013 CIT completed an overhaul of its security and awareness practices around handling of university data. Combined with the elimination of hundreds of thousands of unnecessary
SSNs in various repositories, and a redesign of the business processes that previously required them, this represents a significant reduction in overall risk.

4. The end-user security awareness program has grown considerably in the past two years and now encompasses a wide variety of topics, delivered in both written and video forms. This program has been copied by many of our peers.

5. Campus-wide departmental firewalls were funded for FY15 and FY16, with implementation proceeding throughout calendar 2015. These firewalls will provide custom contemporary threat protection in a manner designed to rapidly adapt to evolving Internet hostility while preserving high-speed, low-latency network connectivity for researchers.

6. A risk assessment of research data and environments was completed by the Office of Sponsored Programs (OSP) in partnership with the ITSO in summer 2014, with the publication of safeguards pending OSP approval. This is the most comprehensive expression of data stewardship thus far at Cornell and represents a significant step toward properly securing research data and environments.

7. CIT and the ITSO have partnered with Environmental Health and Safety to include major security incident response in campus disaster planning.

8. CIT and the ITSO hold quarterly risk management forums to define and prioritize security/risk mitigation investments.


Improving the university’s overall IT security posture requires a combination of senior executive support, targeted technology investment, standalone and integrated security service delivery, policy modernization, a sound policy compliance program, and publishing an adequate set of security safeguards for the research community.

*Contemporary security programs should focus resources in equal measure on prevention, detection, early response, and business continuity.*

Our high-level approach includes:

1. **Investment in centrally delivered security services.** Technologies would be delivered in two broad forms: common-good technologies (protective measures where any barrier to entry creates undue risk) would be incorporated into central services or made available to campus for zero-fee. For-fee security technologies would recoup the cost of the service and represent enhanced capabilities or service levels over common-good counterparts.
   a. **Services would include:** Multifactor authentication tools, commercial data loss prevention tools, upgrades to security log monitoring and alerting tools, security enhancements to CIT private cloud services, vulnerability discovery and remediation, penetration testing, and safe defaults. To establish a secure environment for service delivery, this effort would also include application whitelist, host-based intrusion detection, and other improvements to central virtual machine environments.
   b. **Why these services are critical:** These preventative measures are keys to protecting university data and operations in the current threat landscape. However, these are areas of prevention and detection that have historically been
underfunded in higher-education settings. The industry, our peers, and Cornell are all working toward similar security postures. Investment here is critical.

c. **Timeframe:** FY16 and beyond, with critical safeguards applied to high-risk areas beginning immediately and following throughout calendar 2015.

2. **Policy and standards updates.**

a. **Policy changes needed:** Require multifactor authentication (MFA) for high-risk roles and environments. Extend MFA to departmental environments. Establish baseline security practices for systems holding university or department-level user accounts. Recommend application secure coding standards, vulnerability scanning, and remediation prior to Internet exposure. Require internal or external penetration testing of high-risk environments, at least annually. Require log centralization and analysis, to be combined with privacy policy improvements. Develop a new policy that creates an inventory of administrative data repositories, including owners, provenance, integrations, and security status.

b. **Why:** Processes driven by IT Policy currently address early 2000-vintage threats, rather than the contemporary Internet threat landscape.

c. **Timeframe:** Language changes were created and vetted through the first quarter of calendar 2015. University Policy process consultations will follow immediately, with release by fall 2015. The normal one-year compliance grace period means the affected IT policies will be auditable by the following year.

3. **A policy compliance program, vetted with college leadership, coordinated by the IT Security Office and University Audit.**

a. **What:** A program of compliance checks, awareness, and opportunity notifications to college business officers. Work with Audit to develop an annual audit process for these benchmarks. Work with Risk Management to develop an incentive/disincentive program as related to security incidents and cyber-liability insurance costs.

b. **Why:** Wide deviations from the baselines security standards, even in their current state, significantly undermine the protection of Cornell’s IT assets and reputation.

c. **Timeframe:** Calendar 2015. Discussions with college leadership already underway.

4. **Publish research data security safeguards. Work with the research community through the Office of Sponsored Programs to bring research data security standards to modern levels.**

a. **What:** Promulgate the current set of safeguards. Educate researchers and departmental IT in those requirements.

b. **Why:** Emerging threats to university research data and intellectual property risks competitiveness, prestige, and faculty recruiting.

c. **Timeframe:** As soon as possible, ideally before the end of calendar 2015.

5. **Work with commercial partners to expand and enhance security program.**

a. **What:** Expand the use of commercial penetration testing and security incident response services. Include periodic commercial risk assessments.

b. **Why:** Commercial services allow us to react swiftly to large incidents, ensure a rapid return to optimum IT operations, and capitalize on private sector threat intelligence.

c. **Timeframe:** We have already used Verizon professional services in this area and would work with Verizon and/or other partners over calendar 2015 to increase our capabilities.