Report of the Task Force on Cybersecurity

June 12, 2014

BACKGROUND

On February 18, 2014, it was discovered that a cyber-criminal had breached the University's cybersecurity defenses and had stolen almost 300,000 names, dates of birth and social security numbers that were housed in a file used for ID cards. The penetration that eventually led to this theft was enabled by the presence of an old web site that allowed the uploading of information and had not been updated for eight years. The University quickly responded by transferring all web sites with similar vulnerabilities to the cloud, thereby cutting off access to the University databases containing confidential information.

While the immediate problem was addressed, the data breach served as an urgent reminder that the protection and stewardship of our information and data systems is an issue that affects everyone at the University of Maryland, and that it was time to review our security defenses, in particular those that protect sensitive information such as social security numbers, financial information such as credit card information, passport numbers, taxpayer identification numbers, and passwords, and those that safeguard research data and student records.

As such, President Loh appointed a Task Force on Cybersecurity and charged it to:

1) Find out where sensitive personal information might be located, and to make recommendations as to whether the sensitive data should be purged or protected, and if protected, how should protections be strengthened
2) Perform penetration tests of the security defenses and recommend policies and procedures that establish these probes on an ongoing basis,
3) Review the appropriate balance between Division of IT and unit operated information technology systems, and
4) Consider existing policies and recommend changes or additions as necessary to accompany technical solutions.

This document is the report of that Task Force.

INTRODUCTION

To address these charges, the Task Force divided itself into four subgroups: 1) Security Enhancements chaired by Professor Michael Hicks, Department of Computer Science and member of the Maryland Cybersecurity Center, 2) Policies and Procedures chaired by Director Dan Navarro, Office of Academic Computing Services College of Behavioral and Social Sciences, 3) University Data chaired by Associate Director Michelle Straughn, Undergraduate Admissions, and 4) Penetration testing Chaired by Professor Jonathan Katz, Department of Computer Science and Director of the Maryland Cybersecurity Center. Task

Group members served on one or more groups and other members of the university were added or consulted to enhance experience and expertise with the subgroup topic. The full membership of each subgroup is listed in Appendix A.

METHODOLOGY

The following methodologies were used by the Subgroups and the Task Force to construct this report:

- Review and analysis of the USM proposed standards (Appendix C) , University of Maryland Policy on the Acceptable Use of Information Technology Resources (http://www.it.umd.edu/security/Nethics/Policy/aup.html), the Student Guidelines for Network Computer Use (http://www.it.umd.edu/units/security/Nethics/Policy/network_guidelines.html), University of Maryland Policy on the Collection, Use and Protection of ID numbers (VI-26.00(a) (http://www.president.umd.edu/policies/docs/VI-2600.pdf), University of Maryland Policy on Institutional Data Management http://www.president.umd.edu/policies/docs/vi2200A.pdf) and University of Maryland policy on data management structure and procedures (VI-23.00(a) (http://www.president.umd.edu/policies/docs/VI-2300A_018.pdf)
- Review and analysis of IT Security environments of other institutions of higher education, including those who are members of the Committee on Institutional Cooperation (CIC) (see Appendix B).
- Review of information provided by EDUCAUSE (www.educause.edu)
- Review of the President's Council of Advisors on Science and Technology Report to the President on Immediate Opportunities for strengthening the nation's cybersecurity (www.whitehouse.gov/ostp/pcast)
- Consultation with The MITRE Corporation
- Consultation with Division of IT staff
- Consultation with Steering Committee of the IT Council
- Consultation with the Chair of the Data Policy Advisory Committee
- Consultation with the External Advisory Board of the Maryland Cybersecurity Center
- Development of a list of possible security enhancements
- Penetration Testing. One of our subgroups developed a preliminary scope of work and contacted five companies for their consideration to bid. The group received proposals from four companies, discussed the responses with each company, and determined that InGuardians was highly qualified and had the most experience with higher education of those presenting proposals. They recommended that the University hire them for penetration testing of our central systems. Given the short turn around for this report, it was not possible to test systems not managed centrally, but the report includes recommendations for penetration testing to continue on such systems.

- Identification of points of contact (ultimately, 137 in total) responsible for university data kept by units across the university.
- Survey of these points of contact for any database, system, application or website managed at the unit level that contains date of birth, social security numbers, credit card information, bank information university ID numbers, student grades or letters of recommendation.
- Utilization of the collective expertise of the Task Force and subgroup members

The recommendations included in this report were developed initially by the subgroups. Updates were presented to the full Task Force and reports of the subgroups were circulated among the members for comment. They were then consolidated to form the entire report. They involve policies and procedures, technology and resources, and they are presented in this order. Importantly, they rely on the development of a new tightly functioning network of IT professionals across the campus. While we favor automation in security enhancements when possible, complete automation is not always possible and so some of these recommendations involve additional staff to carry them out. We are mindful of the scarce university resources, so we expect that they may be acted upon over a period of time. We agree, however, that all of the recommendations are necessary to bring the University of Maryland's IT environment to an acceptable level of security and to be in compliance with the USM Security Standards.

Throughout this document, we use the term *confidential information* to include:

1. An individual's first name or first initial and last name, personal mark, or unique biometric or genetic print or image, in combination with one or more of the following data elements:
    a. a social security number;

    b. a driver's license number, state identification card number, or other individual identification number issued by a unit;

    c. a passport number or other identification number issued by the United States government;

    d. an individual taxpayer identification number; or

    e. A financial or other account number, a credit card number, or a debit card number that, in combination with any required security code, access code, or password, would permit access to an individual's account.

2. Educational Records, as defined and when protected by 20 U.S.C. § 1232g; 34 CFR Part 99 (FERPA), in the authoritative system of record for student grades.

3. In addition, any Protected Health Information (PHI), as the term is defined in 45 Code of Federal Regulations 160.103 (HIPAA)

RECOMMENDATIONS ON POLICIES AND PROCEDURES

RECOMMENDATION 1: *Make persistent attention to IT security a top priority for the university and a collaborative responsibility of IT* users and administrators *by creating an IT Security Advisory Committee (ITSAC). ITSAC reports to the IT Council and VP CIO.*

The Task Force recognizes that the ultimate responsibility for IT Security rests with the Vice President for Information Technology and Chief Information Officer (VP CIO). It is his/her responsibility to provide a secure environment for the University's confidential data. Furthermore only the VP CIO has authority to grant access to the University Network. However, to meet these responsibilities and exercise this authority, the VP CIO must have the support and cooperation of the university community.

The University has IT professionals located in many parts of the campus who do not have reporting responsibilities to the VP CIO, yet they deal with confidential, research, and educational data and are responsible for cyber security within their units. Units develop software and systems for their own use. It is important that they can continue to do so: they know their own needs, and local staff who report to them can be quickly responsive. Security can be achieved in cooperation with DivIT if expectations and requirements are clear, and are enforced. This can best be accomplished if there is a systematic process for ensuring communication among this group and involving it in the development and implementation of processes and policies that affect IT security. ITSAC can be a key component of this process.

The ITSAC should have broad representation from colleges and administrative units with separate IT infrastructure and DivIT personnel, including the DivIT Chief Security Officer. The details of the membership should be determined by the Steering Committee of the IT Council. The membership should be inclusive enough to ensure that the needs of UM researchers, administrators and educators are fully represented. The VP CIO through the Chief Security Officer should set up and be responsible for calling meetings of ITSAC. The responsibilities of the ITSAC are outlined in RECOMMENDATION 2 below.

RECOMMENDATION 2: *ITSAC Responsibilities:*

One-time initial responsibilities:

1. *Recommend policies, standards and enforcement mechanisms required for full implementation of and compliance with the Acceptable Use Policy (AUP), the USM IT Security Standards, and the recommendations of the Cybersecurity Task Force (this report).*

   Technology recommendations should be brought to ITSAC for discussion. For example, DivIT may want to mandate that software with known vulnerabilities be phased out within a certain time period or make strong suggestions about secure software choices. A standard that may be considered is to require network activity log aggregation between local IT and DivIT. Standards should be based on those DivIT itself aims to follow. Waivers may be sought and granted by DivIT in some cases and for some periods of time, e.g., if the cost of compliance is currently too high, depending on the data at risk. Certain research data might not be subject to the same requirements as confidential data. For any granted waiver, the unit in question is effectively taking responsibility for any consequences. Of course, DivIT cannot waive its responsibility for protection of sensitive data covered by law or University policy.

2. *Do an initial review of IT policies in place by local departments and compare local IT policies to those in use by DivIT and other sources of best practices.*

3. *Develop a mechanism for periodic review and reporting of operations outside the DivIT on security of systems and applications that store or provide access to confidential data. Procedures for DivIT review and audits of such systems and applications should be reviewed by ITSAC.*

Ongoing responsibilities:

4. *Provide periodic review of the AUP and the Student Guidelines for Network Use to ensure that it effectively serves the evolving IT security needs of the university.*

5. *Provide an on-going review of standards and reports to ensure compliance in the future as technologies evolve.*

6. *Develop a procedure to review security elements and approve procurement of new software used in critical applications.*

   This not only will provide the potential for economies of scale, but it will also provide better interoperability and assist with security since more secure options might be discovered through this process.

7. *Make recommendations on how to address the challenging issues of security of mobile devices.*

   The use of portable devices will continue to increase in the future, presenting complex security problems. Many of these devices will not be institutionally owned. What level of control should the University impose over devices that users wish to connect to the campus wireless network?
8. *Provide advice to DivIT on any other matters that concern IT security.*

RECOMMENDATION 3*: DivIT should enhance security awareness across the University community and provide training.*

Using the AUP as a baseline, DivIT should develop marketing and training materials for all members of the community designed to increase awareness of IT security and the potential negative impacts of security breaches. The training tools should be customized for individuals with access to specific kinds of data, e.g., those which fall under FERPA or HIPPA regulations as opposed to typical users. Mandatory training should be specifically designed for IT staff and other individuals with responsibility for maintaining computers and servers and with responsibility for designing and maintaining websites. In consultation with ITSAC, DivIT should determine appropriate schedules for ongoing training. Working with University Communications, DivIT should also organize periodic University-wide IT Security Awareness campaign.

Security training and awareness are important because even perfect technology can be ineffective when not used properly or can be bypassed altogether if users are unwary. If someone can be tricked into giving up their password, then that information can compromise systems directly. As an institution of learning, we have an obligation to educate our population about security; what they learn will affect their behavior at home, hopefully in a good way. This rationale is consistent with NIST's Recommended Security Controls for Federal Information System and Organizations (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf)
We need to create a culture of security awareness and provide people with the tools for safe computing. For some employees training might be required, but for all, on-line, interactive training customized to the University environment and trainee's role should be available and encouraged. Training should also include best practices for Internet use generally.

Separate training may also be targeted to those more likely to be susceptible to phishing or other social engineering attacks, even if they are not IT staff. Identification of heightened susceptibility must be carried out carefully and fairly. Interestingly, some recent studies have shown that senior managers and executives are an important source of breaches. This is because they have greater access, and more freedom, while not necessarily being any more informed about security risks. For such individuals, expanded training might focus on proper use of UMD-approved software with security in mind, which may shed light on the effectiveness of that software. Development of a web site with best practices, reference material, etc., may be helpful.

RECOMMENDATION 4: *Acceptable use policies, security policies, data management policies, web resources and tools, and security best practices should be very visible, and easy for the average user to find.*

All polices should be reviewed for clarity and policies, best practices, web resources and tools should be placed on a consolidated location on the IT Web site by DivIT.

RECOMMENDATION 5**:** *DivIT, in collaboration with ITSAC, should institute a comprehensive approach to risk assessment.*

There is no such thing as perfect security. As such, we must find a balance that is "good enough" within the resource limits that we can accept. As such, we need to regularly assess our risk in a holistic way, and ensure we are comfortable with the decisions we are making. Such a holistic assessment must consider not only technology, but also users of that technology and the policies that govern that use. Risk assessment must include all sources holding sensitive data: DivIT, units, out-sourced providers (i.e. cloud-based providers) and software service providers from whom we contract the construction of software-based services handling confidential data.

A team within UMD has been working with MITRE to study management practices by which IT risk can be regularly assessed across the institution. The process includes looking at comparable institutions with successful programs, the risk management program at MITRE, and relevant guidance from NIST standards. At the conclusion of the study, the team will issue recommendations on how Maryland's IT Risk Management Program should be implemented.

A formalized IT risk management program should include defining the risk tolerance level for each non-pubic data types, including confidential data and research data. It should also specify mitigations to prevent harm that begin with risks for which there is a low tolerance and specify an exception process that will balance with university business needs. The program should track and report metrics in order to foster awareness for the University leadership.

RECOMENDATION 6: *The Human Subjects Review Committee should require a review by DivIT on the adequacy of the procedures proposed by a principal investigator for the* *protection of confidential human data prior to approval of the research. DivIT could develop standards that if met, satisfy this recommendation.*

Research projects involving human subjects increasingly employ information technology to collect and store data about those subjects, including confidential data. As such, projects must use appropriate technology to protect that data.

RECOMMENDATION 7: *Practice evidence-based security*.

Similarly to the way we determine the effectiveness of a drug in curing a disease or the effectiveness of police departments in reducing crime, we should evaluate the effectiveness of our security policies and protocols in achieving our goals. This evaluation should draw on the collected data, e.g., of network flow data, intrusion-detection and prevent system data (IDS/IPS), incident reports and related user data. Analyses of these data and assessment of what works and what does not will inform our effort to protect our systems from future trespassing incidents. Included in the evaluation should be the impact, if any, on issues of privacy, academic freedom and public access to information.

Evidence-based security is challenging, simply because is not possible to prove a negative, or prove what might have been. Technologies we use will, by definition, be imperfect, so we must expect incidents to occur. What we must assess is whether new technology has improved the situation sufficiently. Has the technology blocked an attack that would have otherwise happened, or reduced the rate of occurrence and the severity of occurrences over what would have been? We should also consider the impact of new processes. For example, we can try to test the effectiveness of training, doing Phishing pen-testing on those who have and have not received anti-Phishing training. A good approach will require careful thought.

RECOMMENDATION 8: *Data retention policies need to be diligently implemented by the Data Policy Advisory Committee (DPAC). Data stewards should ensure that retention policies have been established for the data under their care.*

Data retention policies should be communicated to the community that uses the data. Whenever possible, technology should be employed to automatically remove expired data. Unifying identity management could be useful in this process (See also Recommendation 16).

RECOMMENDATION 9*: Minimize the number of systems, applications, databases and websites that contain confidential data and establish an office of Data Administration within DivIT. This office must ensure that all confidential data are known and securely managed at DPAC-approved locations and that the consistency of data is maintained across systems (this* *will help facilitate business intelligence). It should also provide coordination and facilitate security education for data users and oversee IT privacy issues.*

The Data Policy Advisory Committee, in collaboration with DivIT, should review the databases that contain confidential information and reduce them to the extent possible while enabling secure access to centrally managed databases if the data are necessary.

The Data Subgroup identified over 1500 instances of databases, systems, applications and websites managed at the unit level that contain date of birth, social security numbers, credit card information, bank information, university ID numbers, student grades or letters of recommendation. The survey did not include any sources that are tied into systems that contain confidential data but did not use them directly. A spread sheet containing these data will be provided to DPAC for their review. DPAC may wish to extend this inventory to all databases, systems, applications and websites that are connected to systems that contain confidential data.

Of particular concern to the Task Force are vulnerabilities in systems that 1) process financial aid and admissions and in the process gather and archive documents that contain confidential information, 2) utilize credit card information, 3) process reimbursements, e.g., travel, 4) process payment to vendors, 5) manage personnel matters such as the PHR system, fringe benefit database and the E-Terp system, and 5) record gifts.

RECOMMENDATION 10: *Confidential data should not be stored on portable devices. If absolutely necessary, confidential data must be encrypted.*

Portable devices connected to the university network present a potentially serious risk to the institution. It is difficult to ensure that software on such devices is up to date and that malware is not present. By their very nature, portable devices are easily lost or stolen, which exposes to theft any confidential data they may contain. One way to address this issue is to require that confidential data on all portable devices be encrypted. DivIT should provide free access to encryption training for all available platforms. DivIT should work with ITSAC to develop a process to implement this recommendation.

TECHNICAL RECOMMENDATIONS

RECOMMENDATION 11: *DivIT should ensure the isolation of the confidential data, limit access to it, and log accesses to it,*

1. *Ensuring that firewalls separate sensitive and non-sensitive systems.*

2. *Limiting allowed networking protocols between Internet-facing and internal university systems.*
3. *Requiring VPN-based access for the machines with confidential data, and utilize multi-factor authentication where appropriate.*
4. *Utilizing log aggregation and analysis technologies to improve incident detection and post-incident investigation.* DivIT currently uses log aggregation for some of its systems, but does not aggregate those of systems run by local-level IT.
5. *Educating offices to the risks of using email to transmit sensitive data between individuals and investigating an easy-to-use, more secure alternative.*
6. *Establishing a HIPPA health zone where researcher can transmit, store, manipulate, and analyze research data protected under HIPPA regulations. The environment should provide web capabilities, analytic capabilities, and a backend infrastructure that will protect regulated data and is subject to audit.*
7. *Establishing a Research Data Store (RDS) for researchers who wish to use it.* Research data may contain intellectual property or they may be confidential to a partner. Currently, such data are stored in many places, on many devices, and in many formats, and if not protected sufficiently, exposes the University to risk of reputation, potential loss of collaboration opportunities and loss of property. The RSD should provide a large set of secure storage centrally managed by DivIT and located in the Cyber infrastructure Center, where the data would be available through multiple ways of secure access. Back-up service should also be available for research data located here. The use of the RDS is optional.

These action items aim to support both access control and auditing enabled by logging. Carefully identifying secure data, isolating it, and thoughtfully limiting access to it is important for protecting it from compromises elsewhere in the network, which are inevitable. If a sophisticated compromise or attack to retrieve this data does take place, careful logging is critical for determining what happened.

RECOMMENDATION 12: *Limit exposure and footprint of confidential data by identifying where it is and eliminating data locations not necessary for the specific application.*

DivIT should develop an *implementation plan and provide associated costs for 1) confidential data discovery and 2) desktop and/or application virtualization.*[i]

Through day-to-day usage of email and business systems, it is possible for transient confidential information to take up residence on desktop and laptop computers in data caches and temporary folders. Without a means to discover such data, a computer user might never know that s/he is holding confidential information. The University should broadly support a data discovery tool and require its use on computers that access university business systems. ITSAC should establish policies and procedures to ensure that discovery occurs on regular intervals.

Some confidential data is already isolated, in the sense given above, which limits its exposure. Two more steps are needed. First, we should prevent data from propagating from its source, limiting its exposure *in space*. For example, student application records are stored in the MEGS system, and nowhere else, but these records can spread to the machines of the people that look at applications (e.g., PDFs in their Downloads folder). Further, a reviewer might download from MEGS the personal statement of an applicant. If that machine is compromised or lost, then that private data are exposed. Second, confidential and other sensitive data's exposure should be limited *in time*: it should be deleted as soon as it is no longer needed. In the UMD data breach, literally hundreds of thousands of records were present in the database that did not need to be there in violation of our data retention policy.

Virtualization technology can be used so that users are given a "virtual remote desktop" of a trusted machine. Any interaction with the sensitive data is via that remote machine, and the data stays on that machine. Application-level virtualization is also possible, which is more user-friendly. Examples when virtualization would be advantageous would be access to SIS, MEGS, Hobson admissions software, ID card database.

PDF files may need to be handled specially. One option is to use some form of digital rights management, or only streaming PDF access without a local cache.

RECOMMENDATION 13: *In consultation with ITSAC, DivIT should develop support and technical standards for all network services such as websites, web-based applications, and email.*

DivIT should support and foster developer communities to provide peer support for those responsible for University websites and provide technical advice for those units that do not have the staff to provide adequate support for independently created sites. Once web sites or other network connections are created they may be neglected because of scarcity of staff and financial resources. The recent breach took advantage of an old and outdated web site. Updating and enforcing security standards for web sites, web-based applications, and email must be an ongoing priority for the University to maintain a secure IT environment.

RECOMMENDATION 14: *Use stronger authentication when accessing confidential information by implementing, as appropriate for the risk, 1)two-factor authentication, 2) procedures for restricting access to confidential data by network address, 3) use of VLANS to separate confidential data from research computing, and 4) and development of a process and standards for more stringent password requirements for access to confidential data. Implementation of this recommendation is the responsibility of DivIT in consultation with ITSAC and the IT Council.*

If an adversary steals a user's credentials (e.g., user name and password) s/he can use those credentials to access whatever data the user could access. We should allow users access to information, or change access controls to that information, only if they provide credentials that are difficult to steal and stronger authentication makes compromise harder. These recommendations would provide greater assurance that the user accessing the data is the person expected.

RECOMMENDATION 15: *DivIT must employ state-of-the-art intrusion and malware detection services and systems and continually update them. DivIT should develop and implement a plan for periodic penetration of central systems that use or access sensitive data.*

DivIT in collaboration with local IT system managers should conduct regular (e.g., annual) scans of local systems for private information, e.g., social security numbers and/or credit card numbers. At least annually, reports from Unit IT offices should establish that they are compliant with data retention policies and secure protection of sensitive systems and the data they carry, including the results of a local security audit.

Regular scans and reports will uncover inadvertent or even malicious dissemination of the information. Whether or not scans could sometimes be optional; e.g., for faculty desktops/laptops we make it the faculty member's option to do the scan, should be considered by ITSAC.

Ideally all student and employee records (including SSNs) should be kept centrally. Departments and colleges may want to keep their own confidential data for various reasons, but they should architect their IT in the same way, limiting its exposure. Local maintenance of confidential data must be reported to DivIT and approved by the Data Policy Advisory Committee after consultation with DivIT on appropriate security measures. DivIT must be aware of all local caches of confidential data so that reactions to detected attacks can be tuned appropriately and approve measures for security.

Though not perfect, intrusion and malware detection systems and services help identify and repel some threats. The University already uses intrusion prevention systems at the border of its networks and the Internet. Technology that detects malware internally, that evades border guards, also seems sensible. In addition, implementation of continuously running packet capture at network choke points would facilitate damage assessments in the event of an incident and help to inform legal responses, public relations, and privacy concerns.

The value of penetration testing was demonstrated through a testing engagement with a professional firm selected by the Penetration Testing subgroup. The firm was not able to penetrate core business resources (which provides some measure of confidence about technologies now in place for those resources), but did offer a number of recommendations to reduce risk. The internal network segmentation within the data centers was commended. The firm was successful at identifying vulnerable systems in campus departments and then successfully exploiting those holes to gain control of those computers. The attackers were able to pivot through exposed systems to compromise systems not directly exposed to the Internet. In one case, they were able to uncover a set of documents containing individual PII. Full implementation of recommendations 3, 5, 11, 12, and 13 would have addressed the vulnerabilities that lead to their successful incursions.

RECOMMENDATION 16: *DivIT in conjunction with ITSAC, IT Council, and critical institutional partners including University Human Resources and the Office of the Registrar must establish a unified university-wide identity management framework.*

A university-wide identity management s framework must allow for the quick and efficient creation and modification of the identity and roles of a member of the university community, including external partners. Means must be provided to assure the identity of an individual and then authenticate and authorize one's access to IT resources based on role an individual circumstances. The framework should be flexible enough to meet the needs of individual departments in order to minimize the need for locally based authentication systems. In addition, DivIT should develop procedures to provide Directory IDs for off-campus collaborators to encourage support multi-institution collaborations.

The Strategic Plan for IT outlines a clear need for a robust, flexible, and unified identity management system, while allowing flexibility for local identity management systems where they are essential for technical innovation and research. Widespread adoption of a unified identity management system would help secure the University by reducing the distribution of password stores and facilitating the rapid de-provisioning of services in the event of a termination or account compromise. It is a major project requiring time and resources, but essential for security. A well-architected central identity management architecture should hold one system as authoritative despite appointments, affiliation status or other such relationships with the University. An effort of this sort requires the active participation of a variety of campus stakeholders. Most notable of these would be the offices that manage the enrollment of the vast majority of individuals affiliated with the institution, including faculty, staff and students. More limited deployments of local identity management systems, especially where they could be federated with the centralized system, could reduce the complexity of auditing and managing identities for routine tasks (e.g., moves, adds, and changes) and cybersecurity incident response.

RESOURCE RECOMMENDATIONS

RECOMMENDATION 17*: Increase the number of personnel and budget within the Division of IT to a level sufficient to enable implementation of the security initiatives recommended by the Task Force. DivIT will provide estimates for each recommendation.*

The Task Force recommendations involve technology, people and flexible financial resources. Wherever possible, automation should be employed to enhance security, but this cannot ignore the need for personnel in some cases. There is a temptation to think that pen testing and otherwise "outsourcing" security will work. But since IT moves very fast, it is hard to imagine that periodic scans are going to be sufficient. However, since they are part of the recommendations, this initiative will require resources.

In addition, we need local people with their fingers on the pulse of the University who can handle day-to-day operations, react to incidents as they arise, perform regular tests/evaluations (e.g., locally driven pen testing), support a more secure web environment, implement new technologies such as those that prohibit access to critical systems by devices that do not meet security standards, manage and provide virus protection software if appropriate, ensure compliance with security standards, increase security training and awareness, make recommendations to ITSAC on policies and guidelines, and plan for the future by familiarizing themselves with new technologies and assessing our needs against them. There will also be a ripple effect of any added security requirements; implementation and compliance checking will necessitate more personnel.

On the other hand, cyber-attacks occur far too quickly and too often for humans to be relied on to detect or prevent them all. As such, we must use automated tools, and automate processes that are done manually today. Implementation of recommendations such as virtualization, two-factor authentication, installation of firewalls, etc. will require significant onetime costs. Whether automated or not, resources will be required to implement the recommendations of the Task Force.

RECOMMENDATION 18*: In order to encourage incremental experimentation and rollout, we recommend creating a grant program to support security enhancements in local IT operation.*

Rather than consider only University-wide rollout of all new technologies, it makes sense to perform trials/experiments on a smaller scale. In some cases, small-scale rollout is the only possibility for securing technologies in heavy use in particular departments but not University-wide. The results of small-scale rollout can be significant in and of themselves (by reducing significant overall attack surface) and can be used to inform broader rollout, creating policies and plans for others to follow. Moreover, we should consider ideas from local IT concerning the technologies to use, rather than expecting direction to only come from DivIT.

A grant program would enable a source of funding to enhance security and encourage security innovation at the local level. Local IT units could prepare proposals for the technology to deploy, and promise to perform an assessment along and a detailed plan of deployment for future use, once the work is done. A body within DivIT could judge these proposals based on need, potential impact, and qualifications or some other approach to funding could be adopted.

END NOTES

[i] **Virtualization Primer**

Application Virtualization

Application virtualization allows for an individual application to be made available to a user without having to install the software on that person's local machine. Through a web browser and, typically, a client application, a remote session of the application is run on a server. The actual data/files used by the application and remote session never leave the server, with only the display being visible on the user's machine. Security controls can be set to prevent local copies of the application data, thus limiting the spread of that data. Applications can be made available to only specific active directory groups and managed centrally. These applications are also securely accessible on a variety of platforms (iOS, Android, Linux, and Mac) with none of the data moving to the client's platform.

The School of Engineering, Business, and Geography are currently making use of this technology on campus. Engineering's Service is available to all of campus; cf. http://eit.umd.edu/vcl to see this in action. This implementation does not have restrictions on interacting with the local machines.

Application virtualization is typically licensed on a concurrent user basis; that is, the technology can be available to any number of total users, but only a limited number may use the technology at any given time. A modest installation to support 200 concurrent users would run about $200K initially and then $125K/year recurring (including software, server, and staffing).

In the context of security, application virtualization seems most appropriate for use cases where many people have to interact with the sensitive application for brief periods of time. This also enables securing applications without touching the application.

Desktop Virtualization

Desktop virtualization, also known as VDI (for *Virtual Desktop Infrastructure*), has the same benefits of application virtualization accept an entire machine and its software is made available via a remote desktop. To the user of the remote desktop, it seems as if you are interacting with the machine locally. This enables the applications on the shared machine to share data and provides a familiar experience to the users. You can publish a centrally managed, administrative desktop for sensitive workers. This desktop can be prevented from interacting with the remote user's local environment (e.g., so that files on that remote server cannot be downloaded locally).

Desktop Virtualization is in use on Campus in AGREC, CASL, ARHU, FM and Athletics.
At scale, the cost for a VDI implementation should run between $150-$250/desktop.

In the context of security, this seems most appropriate for use cases where people are spending long periods of time interacting with the sensitive applications.

APPENDIX A

CYBERSECURITY TASKFORCE

Kim L. Colbert	Assistant Director, University Human Resources
Michel Cukier	Associate Professor, Department of Mechanical Engineering; and Director of the Advanced Cybersecurity Experience for Students
Michele Eastman	Assistant President and Chief of Staff
Michael Hicks	Professor, Department of Computer Science
Christian Johnson	Undergraduate Student, Advanced Cybersecurity Experience for Students program
Jonathan Katz	Professor, Department of Computer Science; and Director of Maryland Cybersecurity Center
David Maimon	Assistant Professor, Department of Criminology & Criminal Justice
Dan Navarro	Director of the Office of Academic Computing Services, College of Behavioral and Social Sciences
Porter W. Olsen	Graduate Student, Department of English, Institute for Technology in the Humanities
Terry Roach	Chief Legal Counsel
Apaar Singh	IT Systems Manager, Department of Public Safety
Gerry Sneeringer	IT Security Officer, Division of Information Technology
Michelle L. Straughn	Associate Director, Undergraduate Admissions
Susan Taylor	Professor, Management & Organization Smith School of Business
Amitabh Varshney	Professor, Department of Computer Science; and Director of the Institute for Advanced Computer Studies
Chuck Wilson	Assistant Vice President for Records, Registration and Extended Studies

Ann Wylie	CHAIR TASK FORCE - Professor and Interim Vice President of IT/Chief Information Officer
Jim Zahniser	Executive Director of Information Technology, Clark School of Engineering

SUBGROUP MEMBERS

RobertMaxwell	Security Operations Manager, Division of Information Technology
Kevin Shivers	Senior Security Engineer, Division of Information Technology
Kathy Cavanaugh	Assistant Dean, College of Arts and Humanities
Mike Landavere	IT Director, College of Computer, Mathematical and Natural Sciences
Warren Kelley	Assistant Vice President, Student Affairs
John Zacker	Assistant Vice President, Student Affairs
Jeffrey Hollingsworth	Professor, Department of Computer Science
Erin Howard	Coordinator, Division of Information Technology
Lori Kasamatsu	Coordinator, Division of Information Technology

OTHERS CONSULTED

MITRE	Not-for-profit National Technology Resource
IT Senior Staff	
Michael Brown	Assistant Vice President, Division of Information Technology
Francis LoPresti	Executive Director, Division of Information Technology
Alison Robinson	Assistant Vice President, Division of Information Technology
Tripti Sinha	Assistant Vice President, Division of Information Technology
Phyllis Johnson	Director, Division of Information Technology
Michael Eismeier	Director, Division of Information Technology
IT Council Steering Committee	
Andrew Baden	Professor and Chair, Department of Physics
Paul T. Jaeger	Associate Professor, College of Information Studies
Cynthia Hale	Associate Vice President, Academic Affairs
William Dorland	Professor and Executive Director, Honors College
Jimmy Lin	Associate Professor, College of Information Studies
Jeanne Parker	Assistant Director, Department of Procurement and Supply

APPENDIX B

University	Policy	Ca
Arizona State University	Access to University Technology Resources & Services Policy	
Arizona State University	Information Security Policy	
Arizona State University	Border Firewall Policy	
Arizona State University	Anti-Virus Standard	VI
Arizona State University	Courtesy Affiliate Standard	

Arizona State University	Data Handling Standard	DA
Arizona State University	Data Steward & Trustee Standard	DA
Arizona State University	Incident Response Standard	IN RE
Arizona State University	Peer-to-Peer (P2P) File Transfer / Copyright Infringement Standard	
Arizona State University	Password Standard	PA
Arizona State University	Patch Management Standard	
Arizona State University	PeopleSoft Application Data Trustee Standard	
Arizona State University	Privileged Accounts Standard	
Arizona State University	Risk Assessment and Corrective Action Standard	
Arizona State University	Web Development Standard	W
Arizona State University	Software Development Lifecycle	SD
Arizona State University	Standard Enforcement Exception Request Procedure	
Arizona State University	System Audit Requirements	
Arizona State University	Web Application Security Standard	W
Colgate University	Acceptable Use Policy	AU
Colgate University	Stewardship and custodianship of email	EM
Indiana University	Appropriate Use of Information Technology Resources	
Indiana University	Misuse and Abuse of Information Technology Resources	
Indiana University	Eligibility to Use Information Technology Resources	
Indiana University	Privacy of Electronic Information and Information Technology Resources	
Indiana University	Excessive Use of Information Technology Resources	
Indiana University	Security of Information Technology Resources	
Indiana University	Computer and Network Accounts Administration	
Indiana University	Extending the University Data Network	
Indiana University	Wireless Networking	W
Indiana University	Use of Electronic Mail	EM
Indiana University	Cyber Risk Mitigation Responsibilities	RIS
Indiana University	Web Site Privacy Notices	W
Indiana University	Information and Information System Incident Reporting, Management, and Breach Notification	
Indiana University	Privacy Complaints	
Indiana University	Management of Institutional Data	
Northeastern	Acceptable Use Policy (AUP) (LINK, 2010-02-25)	AU
Northeastern	Written Information Security Program (PDF, 2013)	
Northeastern	InCommon Federation: Participant Operational Practices (PDF, 2012)	
Northeastern	Sponsored Account Policy (Link)	
Northeastern	myNEU Privacy Policy (Link)	
Northeastern	Student Code of Conduct (Link)	
Northeastern	SSN and Personal Information Collection, Handling and Use Procedures (PDF, 2010-02)	DA
Northeastern	Retention and Disposition of University Records Policy(PDF, 2012-05-24)	

Northeastern	Information Disposal Requirements (PDF, 2009-11)	
Northeastern	Identity Theft Prevention Program (PDF, 2009-05)	
Northeastern	Management of Copyright Infringement Complaints (PDF, 2009)	
Ohio State University	Client Computing Security	
Ohio State University	Critical Server Security	
Ohio State University	Web Server Security	W
Ohio State University	Database Server Security	
Ohio State University	Local Administrative Privilege	
Perdue University	Information Security Policy Document Definitions	
Perdue University	Delegation of Administrative Authority and Responsibility	
Perdue University	Authentication and Authorization Policy (VII.B.1)	
Perdue University	User Credentials Standard	
Perdue University	Access Controls Standard	
Texas At Austin	Acceptable Use Policy	AU
Texas At Austin	Computer Crimes Law	
Texas At Austin	Digital Millennium Copyright Act	
Texas At Austin	Enhancing Large Software Purchases (UTS 140)	
Texas At Austin	High Value/High Risk Information Technology Purchase Policy (PDF)	
Texas At Austin	Information Resources Use and Security Policy	
Texas At Austin	Management of UTnet Wireless Access Policy | PDF	W
Texas At Austin	Rate Change Policy | PDF	
Texas At Austin	Releasing Software as Open Source or Contributing Software to Existing Projects Licensed Under the GNU General Public License | PDF	
Texas At Austin	University Data Center Security Policy	
Texas At Austin	University Electronic Mail Student Notification Policy (Use of E-mail for Official Correspondence to Students) | PDF	
Texas At Austin	UT System procedure for Enhancing Large Software Purchases (UTS 140)	
Texas At Austin	Video and CCTV Security Systems	
Texas At Austin	Web Privacy Policy	W
Texas At Austin	Web Accessibility Policy	W
Texas At Austin	Data Classification Standard	DA
Texas At Austin	Minimum Classroom Computing Standards (PDF)	DA
Texas At Austin	Minimum Security Standards for Application Development and Administration	DA
Texas At Austin	Minimum Security Standards for Data Stewardship	DA
Texas At Austin	Minimum Security Standards for Merchant Payment Card Processing	
Texas At Austin	Minimum Security Standards for Systems	SY
Texas At Austin	UT Domain Name System	DO
Texas At Austin	Data Encryption Guidelines	EN
Texas At Austin	Guidelines for Internal Recruiting of UT Austin IT Employees (PDF)	
Texas At Austin	IAM Cloud Integration	
Texas At Austin	Network Monitoring Guidelines	NE
Texas At Austin	University Identification Card Guidelines	

Texas At Austin	Application for Exception from Use of University of Texas at Austin Central Processing Services	
Texas At Austin	Change Management Process	
Texas At Austin	Secure Web Application Coding Guidelines	W
Texas At Austin	Copyright Violations	
Texas At Austin	Extended List of Category-I Data	
Texas At Austin	ITS Copyright Notice	
Texas At Austin	Network Operations Manual	NE
Texas At Austin	Position of Special Trust	
Texas At Austin	Protecting Data on Vulnerable Devices (Security Practices Bulletin #1)	RI
Texas At Austin	Protecting Sensitive Digital Research Data	
Texas At Austin	Server Security Checklists for System Administrators	
Texas At Austin	Security Exception Reporting	
Texas At Austin	University Login Banner	BA
Texas At Austin	Communications System Design, Construction and Commissioning	
Texas At Austin	Grounding and Bonding for Communications	
Texas At Austin	Hangers and Supports for Communications Systems	
Texas At Austin	Conduits and Backboxes for Communications	
Texas At Austin	Cable Trays for Communications Systems	
Texas At Austin	Firestopping Systems for Communications Cabling	
Texas At Austin	Surface Raceways and Boxes for Communications Systems	
Texas At Austin	Identification for Communications Systems	
Texas At Austin	Optical Fiber Testing and Measurement	
Texas At Austin	Copper Testing	
Texas At Austin	Communications Equipment Room Fittings	
Texas At Austin	Communications Entrance Protection	
Texas At Austin	Communications Termination Blocks and Patch Panels	
Texas At Austin	Communications Optical Fiber Backbone Cabling	
Texas At Austin	Communications Copper Horizontal Cable	
Texas At Austin	Communications Faceplates and Modular Jacks	
Texas At Austin	Communications Patch Cords, Station Cords and Cross Connect Wires	
Texas At Austin	Data Communications Wi-Fi Access Points	
Texas At Austin	Campus Security Systems - Design and Construction Standards	
UMD	Acceptable Use Policy	AU
UMD	University of Maryland Policy on Institutional Data Management	
UMD	University of Maryland Policy on Data Management Structure and Procedures	
UMD	University of Maryland Policy on the Acceptable Use of Information Technology Resources	
UMD	University of Maryland Policy on Gramm-Leach-Bliley Act Information Security Act	
UMD	UMCP Policy on the Collection, Use and Protection of ID Numbers	
UNC - Chapel Hill	E-mail Address Policy	EM
UNC - Chapel Hill	E-mail Domain Policy	DO
UNC - Chapel Hill	Incident Management Policy	

UNC - Chapel Hill	Information Security Policy	
UNC - Chapel Hill	Information Security Liaison Policy	
UNC - Chapel Hill	Institutional Data Governance Policy	
UNC - Chapel Hill	Password Policy for General Users	
UNC - Chapel Hill	Password Policy for System and Application Administrators	
UNC - Chapel Hill	Transmission of Protected Health Information and Personal Identifying Information Policy	
UNC - Chapel Hill	Vulnerability Management Policy	RI
UNC - Chapel Hill	Onyen Policy	
UNC - Chapel Hill	Data Network Acceptable Use Policy	AU
UNC - Chapel Hill	Standards for Electronic Media Disposal	
UNC - Chapel Hill	Data Storage Policy	DA
UNC - Chapel Hill	Wireless Networking Policy	W
UNC - Chapel Hill	Copyright Information and Policies	
UNC - Chapel Hill	Mass E-mail Policy	EM
UNC - Chapel Hill	Special Handling for E-mail Accounts	EM
UNC - Chapel Hill	List Server Policy	
UNC - Chapel Hill	Registering Campus IP Addresses	IP
UNC - Chapel Hill	Registering a Non-UNC Domain Name	DO
UNC - Chapel Hill	Wireless Networking Policy	W
UNC - Chapel Hill	Wireless Spectrum Policy	W
UNC - Chapel Hill	Policy on the Privacy of Electronic Information	
UNC - Chapel Hill	HIPAA Information	
University of Chicago	Acceptable Use Policy for Information Technology	AU
University of Chicago	File Sharing Policy	
University of Chicago	New Information Technologies and Intellectual Property at the University	
University of Chicago	Statement on Commercial and Political Use of IT Resources	
University of Chicago	Use of External Service Providers	
University of Chicago	Policy for the Digital Use of the Social Security Number	
University of Chicago	Policy for Use of the ChicagoID	
University of Chicago	Regulated Computer Policy	
University of Chicago	Policy for Authenticating University of Chicago Users	
University of Chicago	Policy On Computer Account and Email Requirements for University Employees	
University of Chicago	Procedure to Handle Requests for Records or Information	
University of Chicago	Use of Non uchicago.edu Domain Names	
University of Chicago	Redirection of University Domain Names to External Networks	
University of Iowa	Acceptable Use of Information Technology Resources	AU
University of Iowa	Social Security Numbers	
University of Iowa	Video Surveillance Policy	VI
University of Iowa	Network Vulnerability Scanning and Penetration Testing	RI
University of Iowa	Enterprise Active Directory	
University of Iowa	Enterprise Password	PA

University of Iowa	IT Security Incident Escalation	IN RE
University of Iowa	UI Residence Halls Network (ResNet)	
University of Iowa	Network Citizenship	
University of Iowa	Mass E-Mail Mailings	EM
University of Iowa	Domain Name Policy	DO
University of Iowa	Email Addresses	EM
University of Iowa	Enterprise Authentication	
University of Iowa	Roles and Responsibilities for Information Security	
University of Iowa	Backup and Recovery Policy	BA
University of Iowa	Information Security Framework Policy	
University of Iowa	Institutional Data Access Policy	DA
University of Iowa	Airspace Policy	
University of Iowa	Computer Data and Media Disposal Policy	
University of Iowa	Computer Security Breach Notification	
University of Iowa	Wireless Networking Policy	W
University of Iowa	Network Address Allocation Policy for IPv4	
University of Iowa	Web Accessibility Policy	W
University of Iowa	Computer Inventory and Internal Control Policy	
University of Iowa	Credit Card Acceptance and Security Policy	
University of Iowa	Enterprise Login ID Standard (HawkID)	
University of Iowa	Computer Security Standard	
University of Iowa	University ID Number Standard	
Univesity of Iowa	IT Development Process	
Virginia Tech	Acceptable use	AU
Virginia Tech	Security and data protection	
Virginia Tech	Identity management	
Virginia Tech	Data administration and transparency	
Virginia Tech	Infrastructure, architecture, and ongoing operations	
Virginia Tech	Project management, acquisition, and deployment	
Virginia Tech	Accessibility	W
Virginia Tech	Acceptable Use and Administration of Computer and Communication Systems	AU
Virginia Tech	Appropriate Use of Electronic Personnel and Payroll Records	
Virginia Tech	Alternate Work Site and Telework Policy	
Virginia Tech	Sales, Solicitation and Advertising on Campus	
Virginia Tech	Use of the Internet and Electronic Communications Systems	AU
Virginia Tech	Acceptable Use of Information Systems at Virginia Tech	
Virginia Tech	Policy for Securing Technology Resources and Services	
Virginia Tech	Safeguarding Nonpublic Customer Information	
Virginia Tech	Policy on Privacy Statements on Virginia Tech Web Sites	
Virginia Tech	Privacy Policy for Employees' Electronic Communications	
Virginia Tech	Policy for Protecting University Information in Digital Form	

Virginia Tech	University Information Technology Security Program	
Virginia Tech	University Information Technology Security Program Standard	
Virginia Tech	Security Standards for Social Security Numbers	
Virginia Tech	Standard for Protecting Sensitive University Information Used in Digital Form	
Virginia Tech	Standard for Securing Web Technology Resources	
Virginia Tech	Standard for Storing and Transmitting Personally Identifying Information	
Virginia Tech	Personal Credentials for Enterprise Electronic Services	
Virginia Tech	PID Procedures: Enterprise Electronic Login Credentials	
Virginia Tech	Standard for Personal Digital Identity Levels of Assurance	
Virginia Tech	Guidelines for Determining the Level of Assurance of Personal Digital Identities	
Virginia Tech	Administrative Data Management and Access Policy	
Virginia Tech	Standard for administrative data management	
Virginia Tech	Interim updates—changes in positions, responsibilities	
Virginia Tech	Information Technology Infrastructure, Architecture, and Ongoing Operations	
Virginia Tech	Standards for Infrastructure, Architecture, and Ongoing Operations	
Virginia Tech	Information Technology Project Management	
Virginia Tech	Policy for the Purchase of Department-Based Computer Systems	
Virginia Tech	Project Management Standards and Procedures	
Virginia Tech	Standard for the Procurement of Information Technology Applications	
Virginia Tech	Information Technology Accessibility	
Virginia Tech	Accessibility Standards	W
Virginia Tech	The Virginia Tech Certification Authority (VTCA)	
Virginia Tech	The Virginia Tech Certification Authority Certificate Policy	
Virginia Tech	Virginia Tech Root Certification Authority Certification Practices Statement	
Virginia Tech	Virginia Tech Server Certification Authority Certification Practices Statement	
Virginia Tech	Middleware Certification Authority	
Virginia Tech	User Certification Authority Certification Practices Statement	