GO COMMITTEE #3
March 31, 2014

MEMORANDUM

March 27, 2014

TO: Government Operations and Fiscal Policy Committee

FROM: Dr. Costis Toregas, Council IT Adviser

SUBJECT: Discussion - Montgomery County Government Cyber Security

ITPCC CIO Subcommittee Membership

Fariba Kassiri, Assistant CAO
Sonny Segal, Chief Information Officer, Department of Technology Services (DTS)
Dieter Klinger, Chief Operating Officer, DTS
Keith Young, County Cyber Security Official

Summary of Staff Recommendations:

There are no recommendations; this is a discussion regarding the cyber security posture of the County. Indeed, parts of the discussion may not be possible without a closed session. However, the Committee will have a chance to review and endorse or modify the Executive's decisions regarding cyber security investments when it takes up the DTS budget on April 7.

Background

On March 14, 2014, the Committee transmitted a letter to the County's CIO (©1-2) expressing concerns regarding the cyber security events currently in the news and raising questions regarding the County's progress in this area. The department has developed a response to these questions (on ©3-10) and a brief presentation on ©11-21. In addition, ©22 is the cover page of the Montgomery County Cyber Security Strategic Plan (CSSP); it is confidential, and a copy is made available to each Committee member under separate cover at the request of the CIO.

Staff remarks

Cyber security is a major concern for all institutions, given the degree to which processes depend on technology platforms and their unhindered operation. Some clear Best Practices are emerging in the field:

- Cyber security is less about compliance to rules and regulations and more about active defense and constant engagement in the issue, with metrics and incentives across the organization.

- Cyber security is not the concern of the technology managers alone, but of the heads of all business lines in an organization. One expert says, "...Cyber threats are not longer a CIO problem, they are a CEO priority".
- Technology protection mechanisms should be arrayed next to management strategies regarding reviews and adaptations of standard business strategies in an era of cyber hacking, and a major emphasis should be placed on employee training in all aspects of cyber security.

One recent, highly publicized case related to a breach in the systems of the University of Maryland, where thousands of records were compromised. The University President, responding to the disastrous headlines and the real continuing threat, issued a memorandum announcing a three-part strategy to be undertaken by a high level Task Force:

> *First, we will scan every database to find out where sensitive personal information might be located. Then, we will either purge it or protect it more fully in that database, as appropriate. There are thousands of databases throughout the campus, many created years ago when the environment for cyber threats was different.*
>
> *Second, we will do penetration tests of the security defenses of our central and local information systems to identify and seal any possible technological gaps through which cyber criminals could get in to search for any information. These probes will be performed on an ongoing basis.*
>
> *Third, we will review the appropriate balance between centralized (University-operated) versus decentralized (unit-operated) IT systems. There must be policy changes to accompany technical fixes. We understand the needs of individual units to control their own servers and databases. We must also ensure that safeguards at central and local levels are equally robust and tightly coordinated. Our University's entire cybersecurity system is only as strong as its weakest link.*

Note that the first step addresses existing IT investments, the second addresses real active steps to secure the system by finding "holes" in the defense, and the third asks an important organizational question regarding the ability to oversee and direct the cyber security investments and strategies across the entire enterprise. These three types of preparations for cyber attacks are relevant to the County today; the CIO is addressing the fit between them and his own plans on ©4. The Committee discussion should focus on these three aspects:

- identifying the risks today;
- actively reducing the risk exposure through continuous testing; and
- Reviewing the balance between centralized and decentralized cyber security strategies in the County.

MONTGOMERY COUNTY COUNCIL
ROCKVILLE, MARYLAND

MEMORANDUM

March 14, 2014

TO: Sonny Segal, Chief Information Officer
Department of Technology Services (DTS)

FROM: Councilmember Nancy Navarro, Chair
Councilmember Cherri Branson
Councilmember Hans Riemer
Government Operations and Fiscal Policy Committee

RE: Cybersecurity Strategic Plan

As you know, the Council's Government Operations and Fiscal Policy Committee oversees the Department of Technology Services, and the Committee is scheduled to review the County's Cybersecurity Strategic Plan on March 31.

We are all well aware that cyber attacks pose a very serious threat. In addition to highly publicized attacks like the Target breach, the Identify Theft Resource Center reports that there have already been 130 major data breaches in 2014 which exposed more than 2.8 million records. That number includes breaches of state government systems in Iowa, Oregon, California, Connecticut, North Carolina, and South Carolina and systems operated by the City of Detroit and the Memphis Police Department. It is not a question of *if* Montgomery County government will be targeted, but *when.*

Of course, the only way to be 100% certain we will never be breached would be for the County to cease providing any of the services that require us to collect and store confidential information. As long as we use computers to accept credit cards for parking, help residents obtain health care, investigate crimes, or perform almost any other government function, the County will be a target. We also have limited resources - even if we devoted our entire budget to cybersecurity there would still be more we could do. As Councilmembers, our #1 job is to craft a budget which stretches our limited resources

STELLA B. WERNER COUNCIL OFFICE BUILDING • ROCKVILLE, MARYLAND 20850
(240) 777-7968 • TTY (240) 777-7914
COUNCILMEMBER.NAVARRO@MONTGOMERYCOUNTYMD.GOV • WWW.COUNCILMEMBERNAVARRO.COM

to meet as many of the needs of our community as possible.

At the same time, we are not cybersecurity experts. We rely on documents like the Cybersecurity Strategic Plan to collect and distill the consensus of the highly trained IT professionals employed at DTS and across County government. We are looking to you to provide a comprehensive analysis of the risks we face and the actionable steps we can take to protect ourselves. The Strategic Plan should be a roadmap that prioritizes how we protect ourselves so that we fix our biggest weaknesses first. To do this effectively, it must include performance measures and a timetable. If necessary, the Committee can hold a closed session regarding sensitive security elements that would be inappropriate for public discussion.

When the University of Maryland suffered a data breach, University President Wallace Loh identified three top priorities to secure the University's systems going forward: a comprehensive scan and indexing of where sensitive data was located on the University's systems, penetration testing of the systems to identify weaknesses, and a review of whether systems should be under centralized or decentralized control. At the March 31 meeting, please be prepared to discuss whether the County has taken similar steps to secure our infrastructure and what our top priorities should be going forward. When the Committee reviews the Department's budget in the coming months, we expect to use the Strategic Plan to determine whether the Executive's recommendations address our highest priorities.

CC: Fariba Kassiri, Assistant Chief Administrative Officer
Dieter Klinger, Chief Operating Officer, Department of Technology Services
Costis Toregas, Council IT Advisor
Justina Ferber, Council Legislative Analyst
Councilmembers

STELLA B. WERNER COUNCIL OFFICE BUILDING • ROCKVILLE, MARYLAND 20850
(240) 777-7968 • TTY (240) 777-7914
COUNCILMEMBER.NAVARRO@MONTGOMERYCOUNTYMD.GOV • WWW.COUNCILMEMBERNAVARRO.COM

Montgomery County Government
Cybersecurity Briefing
March 31, 2014

The scope of this briefing is to:

1. Review recent cybersecurity developments
2. Discuss the University of Maryland's Breach Response Plan
3. Convey the high level scope of the County's program
4. Discuss the high level status of the County's program
5. Discuss high level work plan roadmap
6. Identify items of further interest to the GO Committee
7. Identify next steps in providing the identified items

1. Recent Cybersecurity Developments

Cybersecurity breaches occur all the time given the rapidly evolving cybersecurity threat landscape described at length in the draft Cybersecurity Strategic Plan (CSSP) dated February 2014. Valuable lessons are learned from each breach. Two prominent cybersecurity breaches occurred recently; one at the University of Maryland and a second at the Target Corporation. Both these provide valuable insight to cybersecurity specialists.

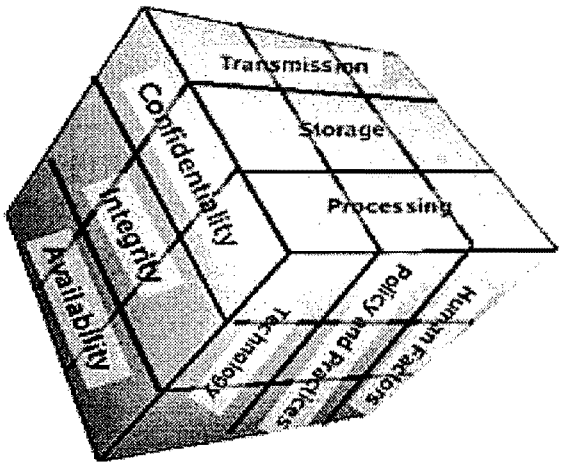
In February 2014, the University of Maryland (UMD) reported a major database breach. The background is that in the 1990's, the University began using university identification numbers instead of social security numbers, but retained the SSNs so former students could request transcripts and other records. Reportedly these historical records were not secured as well as the University's current records but their release adversely affected several thousand people.

In December 2013, Target Corporation announced that a cyber intruder had gained access to credit card numbers used at their stores over the previous month. As unlikely as it seems, the attack was performed through a third-party heating and air conditioning maintenance contractor utilized by the company.

These are clearly security breaches. By comparison, inadvertent release of certain sensitive information by staff is classified by security experts as a security incident.

Gartner Corporation, one of the County's advisors on information technology governance emphasizes that the lessons learned from these breaches do not warrant an overly reactive response but a careful review of any organization's cybersecurity program. Gartner further states that cybersecurity programs should not be reactionary but be designed to gradually improve the maturity of an organization's cyber security defenses. This implies that a number of things have to happen. As an example, cybersecurity has to become ingrained in the culture of an organization addressing all the elements labeled in GWU's Prof. John McCumber's Cube in Figure 1 below.

Figure 1: McCumber's Cube



The McCumber model reminds us to consider all important design aspects of a security program without becoming too focused on any one aspect in particular. As an example, relying exclusively on technical controls at the expense of requisite policies and end-user training can increase risk. Operationally, the one singular aspect of the model that stands out is Availability. Availability refers to an organization's information (i.e., derived from data and systems) on which it depends to successfully operate its business. The implication is that while addressing the other factors in the cube one has to be careful and not affect the organization's ability to conduct business in a cost effective manner. This requires organizations to make security decisions that lower risk but do not degrade system and infrastructure performance, greatly overrun information technology (IT) budgets, and result in customer/constituent/user dissatisfaction.

Prior to the announcement of the reactionary, ambitious and simplified cybersecurity action plan laid out by the UMD President for the next 90 days, the Department of Technology Services (DTS) reviewed the County's cybersecurity program which resulted in the County Executive's recommendation to County Council that additional resources be added to the DTS budget in FY14 and FY15 to further strengthen the security program. Needless to say, if deemed necessary, the County's cybersecurity program can be further accelerated.

2. Status of Items in UMD's Response Plan

The section below on the following bullets address items in Ms. Navarro's letter dated March 14, 2014, that are in the UMD President's breach response plan:

- The efforts to identify sensitive data in the County's systems is ongoing
- The FY15 Recommended Budget includes funding to conduct penetration testing of high risk assets
- The next meeting of the IPAC is dedicated to security and the agenda includes discussion of security governance

3. High Level Scope of the Cybersecurity Program

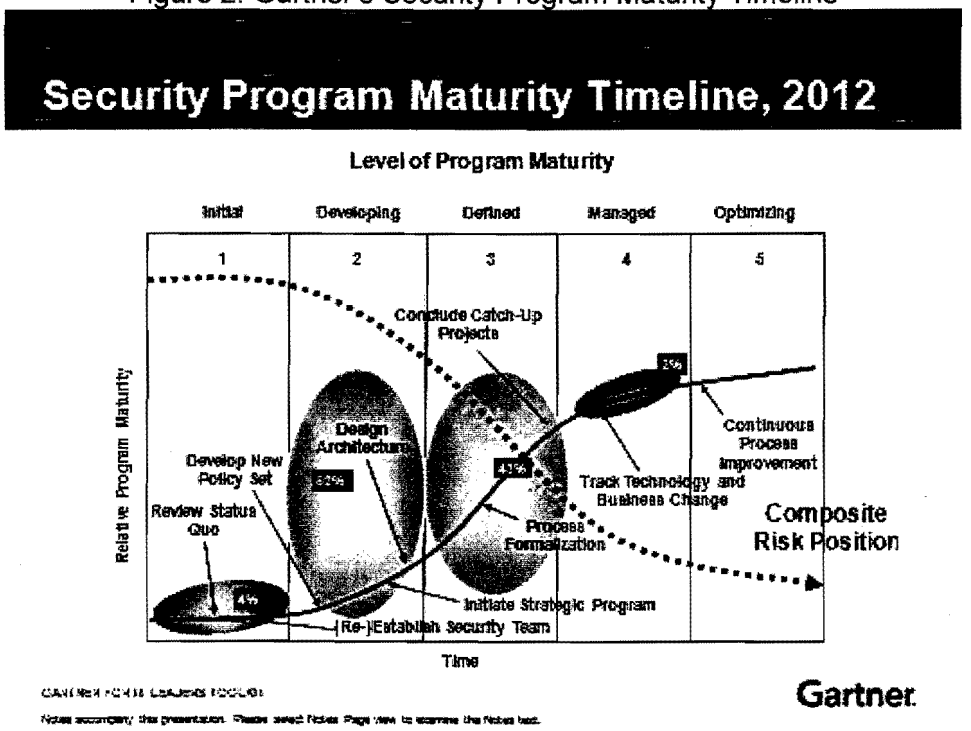
The County's cybersecurity program is continually maturing to manage evolving cyber security risks. This maturation is an ongoing process based on the threats, resources allocated to it, and prioritization given to it. Current maturity falls well within the majority of the security programs in

Gartner's Security Program Maturity Timeline shown in Figure 2.

This figure illustrates the Gartner Security Program Maturity Curve. The lower left represents organizations that are technology-focused and reactive to security issues. The upper right represents organizations that are process-oriented and proactive that can take advantage of efficiencies to provide better protection at lower cost. The black arrows represent the milestones that an organization hits as its maturity improves. The large bubbles represent the percentages of organizations in the Gartner client base at different levels of maturity in 2012.

Like all organizations, information security management at Montgomery County is based on a structure of both risk management and legal compliance. Information security risk management is a function of three elements: people, processes, and technology. In order to lower risk and improve security, enhancements must be made in each of those three areas simultaneously; if those three elements become unbalanced, information security risk is then significantly increased. As the classic proverb states, "[information security] is only as strong as its weakest link".

Figure 2: Gartner's Security Program Maturity Timeline



Even in stages 4 and 5, complete security is not guaranteed. Each organization must invest in security controls commensurate with the perceived potential risks to operation, liability, non-compliance with the law, and cost. The County must make trade-offs on information security protection versus cost and convenience. Because a completely secure organization is impossible, these trade-offs cannot ever eliminate risk, but are instead designed to manage risk to an appropriate level and reduce the risk of a breach and minimize its impact to the County and its data.

One important aspect of the County's cybersecurity program is the protection of its data. This includes all types of data including personal (e.g., constituent, employee), business (e.g., contractors, on-line payers, business partners) and financial data. Protection of data is governed by several laws. In making data security decisions, the Security and Privacy Officers and their programs work closely together.

(5)

The Maryland Public Information Act ("MPIA") defines how Montgomery County classifies the data contained within our information systems. Under the MPIA, data can either be made public, can be classified as sensitive, or is superseded by information security requirements in other Federal, State, or County laws.

Confidential data is data required by Federal, State, or County law not be disclosed to the public. All confidential data must be secured from unintentional disclosure or loss by employees and departments. Some examples of confidential data under the MPIA, are personally identifiable healthcare information, student information, personnel records, an individual's financial information, and social security numbers. Additional examples of confidential information under the MPIA are information about the County's computer security and facilities security, confidential commercial or financial information, some criminal justice data, and information reflecting executive decision-making processes.

Data that is regulated by other laws, including the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Maryland Security and Protection of Information Act, and the Payment Card Industry Data Security Standard ("PCI DSS"), require specific controls when that data is processed by organizations. In the case of the PCI DSS, over 250 very specific technical, operational, and managerial controls must be put in place to protect the handling of credit card information. The County must focus on protecting this data. Failure to do so could result in fines or other sanctions.

The following three levels of classifications must be examined when designing security protections around people, processes, and technologies:

- Data that is made public should not have weak security protections in place. Such examples include the County's Open Data initiative or publicly-posted Council packets.
- Sensitive Data, such as personnel records, are governed by the MPIA and must be protected from release. The County must utilize risk management methodologies in order to protect the information to a reasonable level from breach or loss.
- Regulated Data requires the specific controls to be instituted. These controls can be expensive to implement and, in many cases, would not be cost-effective to deploy across the entire enterprise. They must be applied selectively and be re-evaluated continually.

The County's rules of behavior regarding the handling of sensitive data are included in its mandatory Security Awareness training program.

Cyber security maturity planning should be treated very similarly to disaster recovery planning for natural disasters. The frequency, nature and scale are unknowns however reasonable efforts must continually be made to be able to recover with the least possible loss of data confidentiality and integrity and operational capability. Discussion regarding the specific types of technical controls is best suited for a closed session.

The following sections convey the high level state of the County's cybersecurity program and readiness.

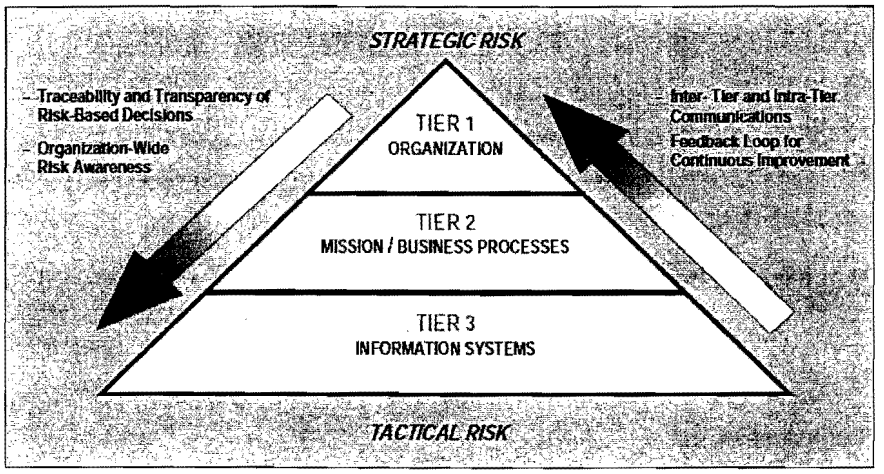
4. High Level Status of the Cybersecurity Program

In order to validate and benchmark its cybersecurity practices against other leading jurisdictions, the County participates in third-party benchmarking studies and security audits. We also continually evaluate and strengthen the program by allocating additional resources to security initiatives and tasks.

Governance

As shown in Figure 3, and discussed at length in the draft CSSP, the County's cybersecurity program is governed at three levels covering policy, technology and operations. The Enterprise Information Security Office (EISO) team in DTS is responsible for formulating and recommending security policy and controls as well as providing security awareness training. The IT Policy Advisory Committee (IPAC) chaired by the Chief Information Officer (CIO) review security policy, organizational and operational issues that affect the Federated (decentralized) IT environment. The IPAC makes recommendations to the Chief Administrative Officer (CAO).

Figure 3: Security Program Governance Structure (NIST)



It takes many personnel in IT functions, including those in DTS and those in the departments, to implement and administer security policies and controls. Many members of the Technology Operations Management Group (TOMG) and the interdepartmental Security Committee, chaired by the County's Security Official, are the same. These groups work with DTS to implement security policy, raise security awareness, and respond to security and privacy incidents. This security governance structure is designed to ensure everyone understands that security is their responsibility too and it serves well.

To detect and deal with constantly evolving cybersecurity attacks and threats in real time, the County's EISO team stays connected at all times with many listening posts and information gathering organizations at the national, state and regional levels. In addition, the County's Security Official is a member of the Metropolitan Washington Council of Governments (MWCOG) Cybersecurity Officials Committee. In addition, the Security Officers of the County's external agencies are members of a Security Working Group of the CIO Subcommittee of the Interagency Technology Policy Coordinating Committee (ITPCC) which is comprised of the heads of all County agencies and the County's CAO. All these organizations have the potential for performing as mutual aid partners in case of a cybersecurity disaster. The County's Security Official, CIO, COO and IT operations managers keep abreast of evolving trends in operational security and risk management.

Threat Landscape

Sources of cyber security risks abound in nearly all organizations - not just the County – due to many environmental factors and trends. Cyber security risks have changed from purely "bits and bytes" to a combination of human, business, regulatory, and technical threats.

The County faces several critical business challenges and security threats:

- The County's investment in technology in its internal functions increases its exposure to cyber threat.
- Due to cost, familiarity, and extensibility, County staff is adopting the use of consumer device and application technologies for business use. These solutions are cheaper (even "free") than their traditional centralized IT counterparts and, in many cases, provide greater features and extensibility.
- The County's desire to maintain close constituent contact and partner relationships have caused an increase in the use of online services, collaboration, and open data. As a result, the County has a greater utilization of online services by citizens, business partners, and other jurisdictions.
- There is a broader trend of increasingly more targeted cyber-attacks against VIPs and government leaders in both public and private sectors. The County's program must take this trend into account.
- Groups of ill-intentioned hackers and civic activists essentially acting as digital terrorists ("hacktivists") are teaming up to disrupt government services when their demands are not met. The County's program must take this trend into account.
- The public has grown increasingly concerned over information security and breach announcements. The severity of breaches has grown and employees, constituents, taxpayers and officials want to be continually assured their information and funds are safe.

The County's cyber security program must keep up with these demands and incorporate cybersecurity review and controls in every new service it plans to implement.

Cybersecurity Strategies

The draft CSSP lists several strategies developed to not only counteract the known and future threats, but also to encourage continued government innovation and enhance cost efficiencies.

These strategies are as follows:

- Continue to enhance the use of secure and stable cloud technologies - adopt new cloud technologies and safely allow non-enterprise applications and technologies (e.g., Square, Uber, Prezi).

- Secure County data on legacy and next generation devices - protect existing desktop/laptop infrastructure along with next-generation Bring Your Own mobile devices and technologies.

- Manage users of all County services, systems, and applications - institute policies to identify and manage citizen, business partner, volunteer, and employee access to all County online services, both in the cloud and in traditional

software applications.

- Assess requirements and recommend reasonable risk solutions - evaluate and correct existing compliance gaps and suggest rational controls for new standalone IT projects.

- Modify enterprise user behavior to improve overall security/privacy posture - change the security mindset of individuals through enhanced and regular training, updated policies, and increased enforcement of policy adherence.

- Streamline and automate security - accelerate automation of security tools and processes in order to reduce costs and increase security visibility throughout the infrastructure and business processes.

Major Program Activity Areas

At a high level, the County's cybersecurity program maintains initiatives in the following areas:

- Project Management
- Enterprise Architecture
- Risk Assessment
- Information Security Compliance
- Incident Reporting and Response
- Computer Forensics and eDiscovery
- Vulnerability Management
- End-user security awareness
- Host Security Management
- Perimeter Network Security
- Asset management and retirement
- Continuity of Operations (COOP) and Disaster Recovery (DR) Planning

If an acceleration of the County's cybersecurity program is desired, more details about the activities in the program can be presented.

5. High Level Work Plan Roadmap

The chart in Figure 4 is a high level roadmap that categorizes high level work plan items by cost and stages them as short, medium and long-term items.

6. Items of further interest

7. Next steps

Figure 4: High Level Roadmap*

	Short Term	***Medium Term***	***Long Term***
Low Cost (<$50k)	-Program Benchmark Assessment -IPAC/TOMG/SC Engagement (Organization review) -Security awareness expansion	-Program Maturity Assessment -Employee rules of behavior -IPAC/TOMG/SC Engagement -CyberSecurity Awareness Month event -Architecture review/update	-IPAC/TOMG/SC Engagement -Architecture review/update
Medium Cost ($50-150k)	-Incident response -Security awareness training -Large project IT system assessments -Policy Update -Automated security tools -Patch management -Major Systems Audit	-Incident response -Security awareness training -Cloud security framework -Policy Update -Identity Management Improvements -Comprehensive Policy Review -Security Executive dashboard -Application Virtualization (APP-V) -Large project IT system assessments -Automated security tools -Patch management -Major Systems Audit	-Incident response -Security awareness training -Enhanced user monitoring -3rd party assessment framework -Large project IT system assessments -Automated security tools -Patch management -Major Systems Audit
Higher Cost (> $150k)	-End point vulnerability -Migrate office and collaboration to cloud -Ongoing regulatory compliance -Enterprise Risk Assessment -Penetration Testing/Risk Assessment -Asset replacements -Perimeter security upgrades -PC management upgrades -Identity Management expansion and automation -COTS Vulnerability Management	-Enterprise Risk Assessment -Ongoing regulatory compliance -Asset replacements -Virtual Desktop Infrastructure (VDI) -Mobile Device Management (MDM) -Identity Management expansion and automation -Application vulnerability remediation -COTS Vulnerability Management -Penetration Testing/Risk Assessment	-Penetration Testing/Risk Assessment -Strong Authentication -Ongoing regulatory compliance -Continued build-out and automation of incident response capabilities -Identity Management expansion and automation -COOP & DR Upgrade -COTS Vulnerability Management

*Timeframes are dependent on government priority, resources and funding.

(10)

Department of Technology Services
DTS
eGov@work!

Montgomery County Government Cybersecurity Briefing

To

GO Committee

March 31, 2014

Department of Technology Services
DTS
eGov@work!

SCOPE OF BRIEFING

- Review recent cybersecurity developments
- Discuss the University of Maryland's breach response plan
- Convey the high level scope of the County's program
- Discuss the high level status of the County's program
- Discuss high level work plan roadmap
- Identify items of further interest to the GO Committee
- Identify next steps

(2)

RECENT CYBERSECURITY EVENTS

- February 2014 - The University of Maryland reported a major database breach. In the 1990's, the University began using university identification numbers instead of social security numbers, but retained SSNs so former students could request transcripts and other records.
- December 2013 – Target announced a cyber intruder had gained access to credit card numbers used at their stores over the previous month. The attack was performed through a 3rd-party heating and air conditioning maintenance contractor utilized by Target.
- OHR incident
- Increasingly, targeted attacks are occurring against VIPs and government leaders in both public and private sectors.

(13)

UMD'S ACTION PLAN ITEMS

UMD's Items

- Comprehensive scan and indexing of where sensitive data was located on the University's systems
- Penetration testing of the systems to identify weaknesses
- Review of whether systems should be under centralized or decentralized control.

Status

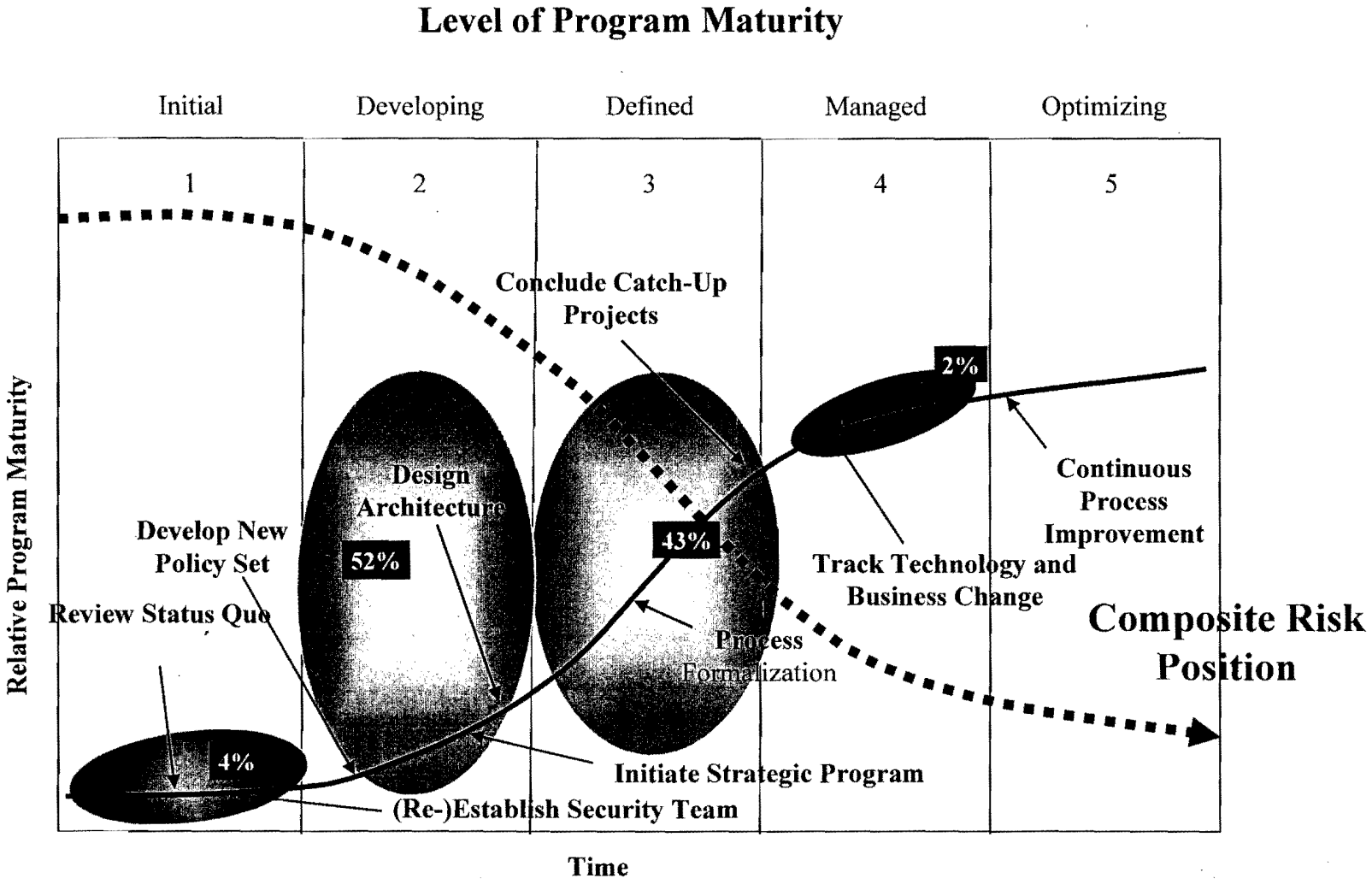
- The efforts to identify sensitive data in the County's systems is ongoing
- The FY15 Recommended Budget includes funding to conduct penetration testing of high risk assets
- The April 1, 2014 meeting of the IPAC is dedicated to security and the agenda includes discussion on security governance

MONTGOMERY COUNTY – CYBERSECURITY PROGRAM MATURITY

- Cybersecurity Maturity assesses the strength and vulnerability of an organization across people, process, and technology.
- DTS has engaged the Corporate Executive Board to perform a Cybersecurity Maturity Framework Assessment. The assessment will:
  - Provide a snapshot of the maturity levels of the County's security controls.
  - Compare Montgomery County's security process maturity versus 300 other entities.
  - Enhance prioritization of budget investment to align with the greatest security process needs.
  - The completed assessment will available in April 2014.

(15)

SECURITY PROGRAM MATURITY TIMELINE, 2012



Source: Gartner, Inc.

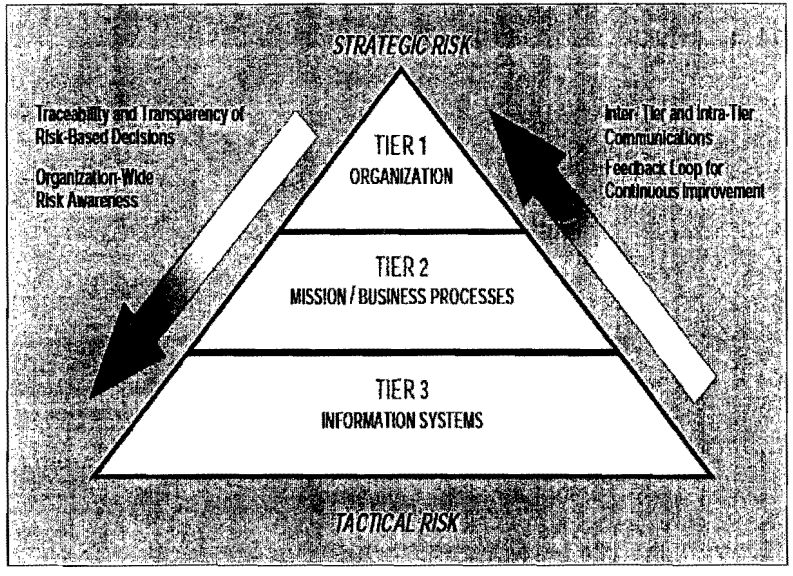
(16)

MONTGOMERY COUNTY – SECURITY / BUSINESS CHALLENGES

- **Breaches will occur** – The County's security goal is to:
  - Contain the breach and minimize impact
  - Increase compliance with security controls and policy to minimize security vulnerabilities
  - Balance security protection with business convenience and cost
- **The County's cybersecurity program is continuously innovating to meet evolving business needs and security challenges**
  - The County's forward-looking cybersecurity program is imperative to ensure consumer confidence in government online services.
  - The County's cybersecurity program is evolving to continue to ensure secure use of cloud services and security of Bring Your Own mobile devices, applications and technologies (*e.g.*, Square, Uber, Prezi).
  - The County is continuously enhancing its incident detection processes to improve overall security and protection of sensitive data.

MONTGOMERY COUNTY – CYBERSECURITY PROGRAM

- **The County's Cybersecurity Program is maturing to manage evolving cyber security risks.**
- **Montgomery County Cybersecurity Strategies FY2014-2017**
  - Continue to Enhance the Use of Secure and Stable Cloud Technologies
  - Secure County Data on Legacy and Next Generation Devices
  - Manage Users of All County Services, Systems, and Applications
  - Assess Requirements and Recommend Reasonable Risk Solutions
  - Modify Enterprise User Behavior to Improve Overall Security and Privacy Posture
  - Streamline and Automate Security



(18)

Department of Technology Services
DTS eGov@work!

MONTGOMERY COUNTY – SECURITY AWARENESS TRAINING UPDATE

- People are the first line of defense against security threats.
  - This includes employees, business partners, contractors, constituents
- Security awareness training is critical and mandated by different laws and regulations (*e.g.*, HIPAA, PCI).
- On-line training will be augmented by reminders, classroom training and remedial training.
- A "security first" culture must be achieved in order to improve the security posture.

(19)

MONTGOMERY COUNTY – HIGH LEVEL ROADMAP

	Short Term	*Medium Term*	*Long Term*
Low Cost (<$50k)	-Program Benchmark Assessment -IPAC/TOMG/SC Engagement (Organization review) -Security awareness expansion	-Program Maturity Assessment -Employee rules of behavior -IPAC/TOMG/SC Engagement -CyberSecurity Awareness Month event -Architecture review/update	-IPAC/TOMG/SC Engagement -Architecture review/update
Medium Cost ($50-150k)	-Incident response -Security awareness training -Large project IT system assessments -Policy Update -Automated security tools -Patch management -Major Systems Audit	-Incident response -Security awareness training -Cloud security framework -Policy Update -Identity Management Improvements -Comprehensive Policy Review -Security Executive dashboard -Application Virtualization (APP-V) -Large project IT system assessments -Automated security tools -Patch management -Major Systems Audit	-Incident response -Security awareness training -Enhanced user monitoring -3rd party assessment framework -Large project IT system assessments -Automated security tools -Patch management -Major Systems Audit
Higher Cost (> $150k)	-End point vulnerability -Migrate office and collaboration to cloud -Ongoing regulatory compliance -Enterprise Risk Assessment -Penetration Testing/Risk Assessment -Asset replacements -Perimeter security upgrades -PC management upgrades -Identity Management expansion and automation -COTS Vulnerability Management	-Enterprise Risk Assessment -Ongoing regulatory compliance -Asset replacements -Virtual Desktop Infrastructure (VDI) -Mobile Device Management (MDM) -Identity Management expansion and automation -Application vulnerability remediation -COTS Vulnerability Management -Penetration Testing/Risk Assessment	-Penetration Testing/Risk Assessment -Strong Authentication -Ongoing regulatory compliance -Continued build-out and automation of incident response capabilities -Identity Management expansion and automation -COOP & DR Upgrade -COTS Vulnerability Management

*Timeframes are dependent on government priority, resources and funding.

(8)

MONTGOMERY COUNTY – SUMMARY

- County Council support for the County Executive's Recommended $280,000 increase for cybersecurity in the DTS Budget will enhance the County's cybersecurity program.
- Corporate Executive Board's Cybersecurity Maturity Framework Assessment is expected to be delivered in April 2014.
- Security awareness training is on pace to meet goal of having all employees and contractors trained in the short term.

(12)

	**Montgomery County Maryland** **Strategic Plan for Enterprise Security and Information Risk Management**
	Fiscal Years 2014 - 2017

Department of Technology Services

February 2014

This draft document is for internal review only and is subject to change.

It is not intended for release outside County government.