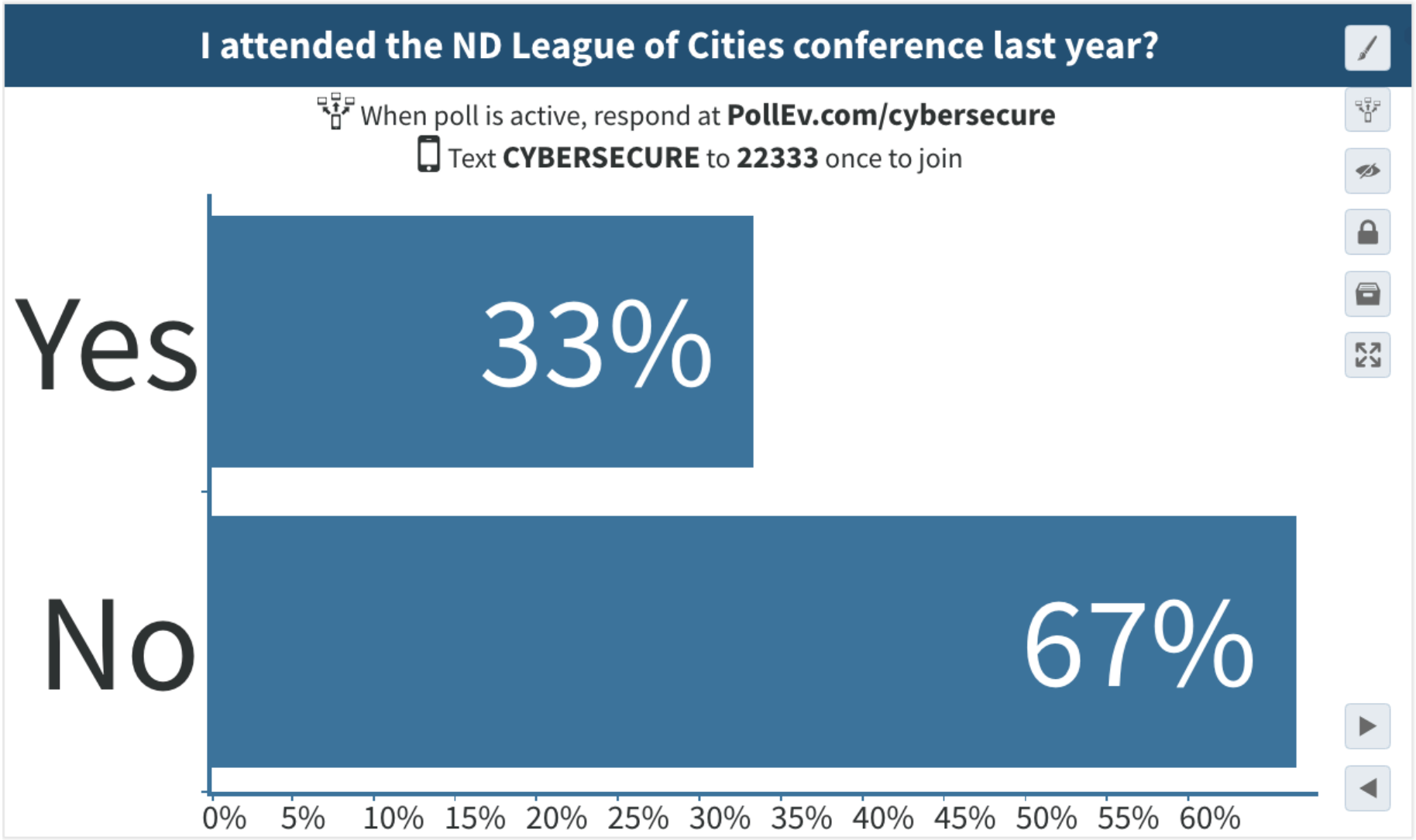
NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Cyber Security Issues

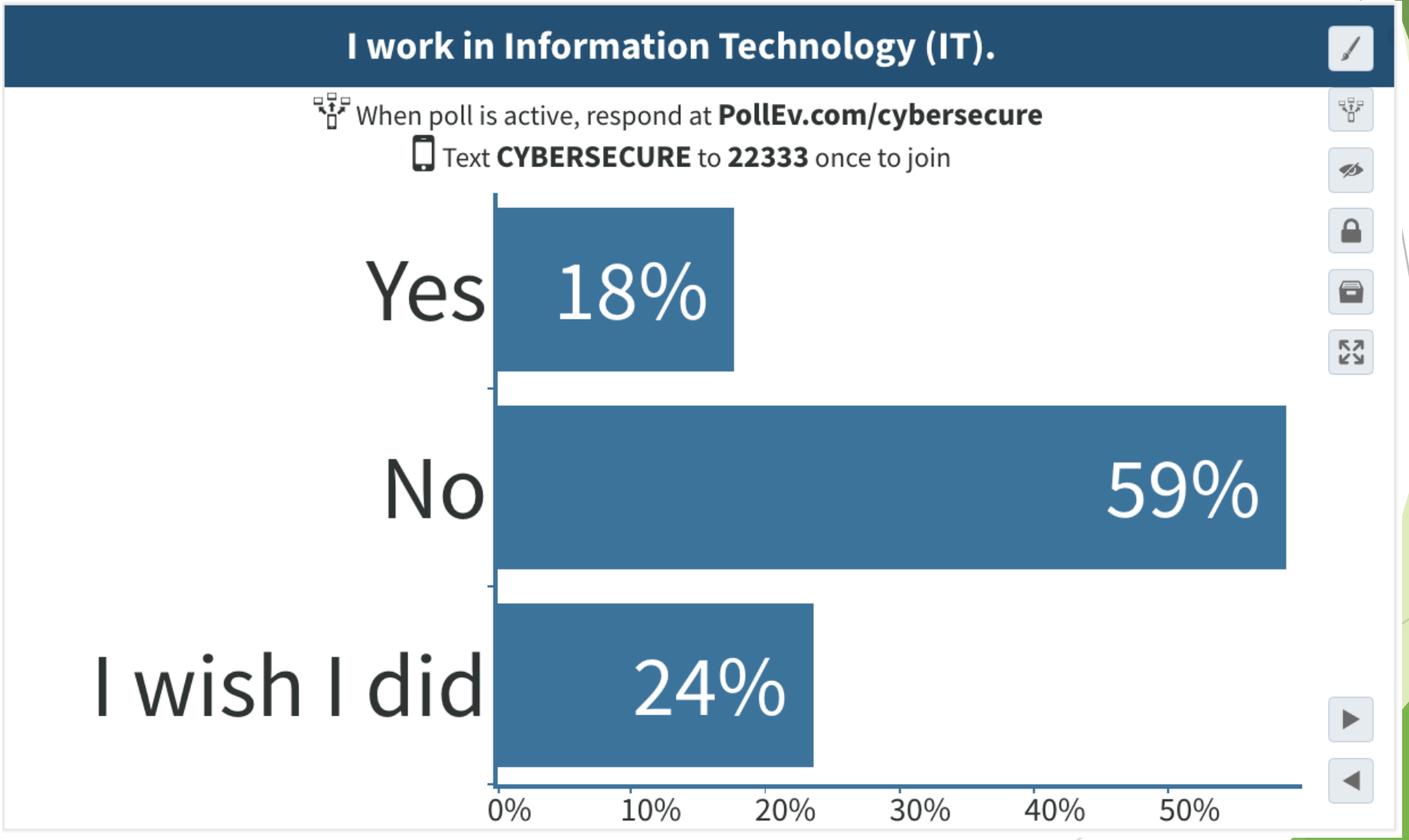
Brad Miller

NDUS Director of Information Security

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.



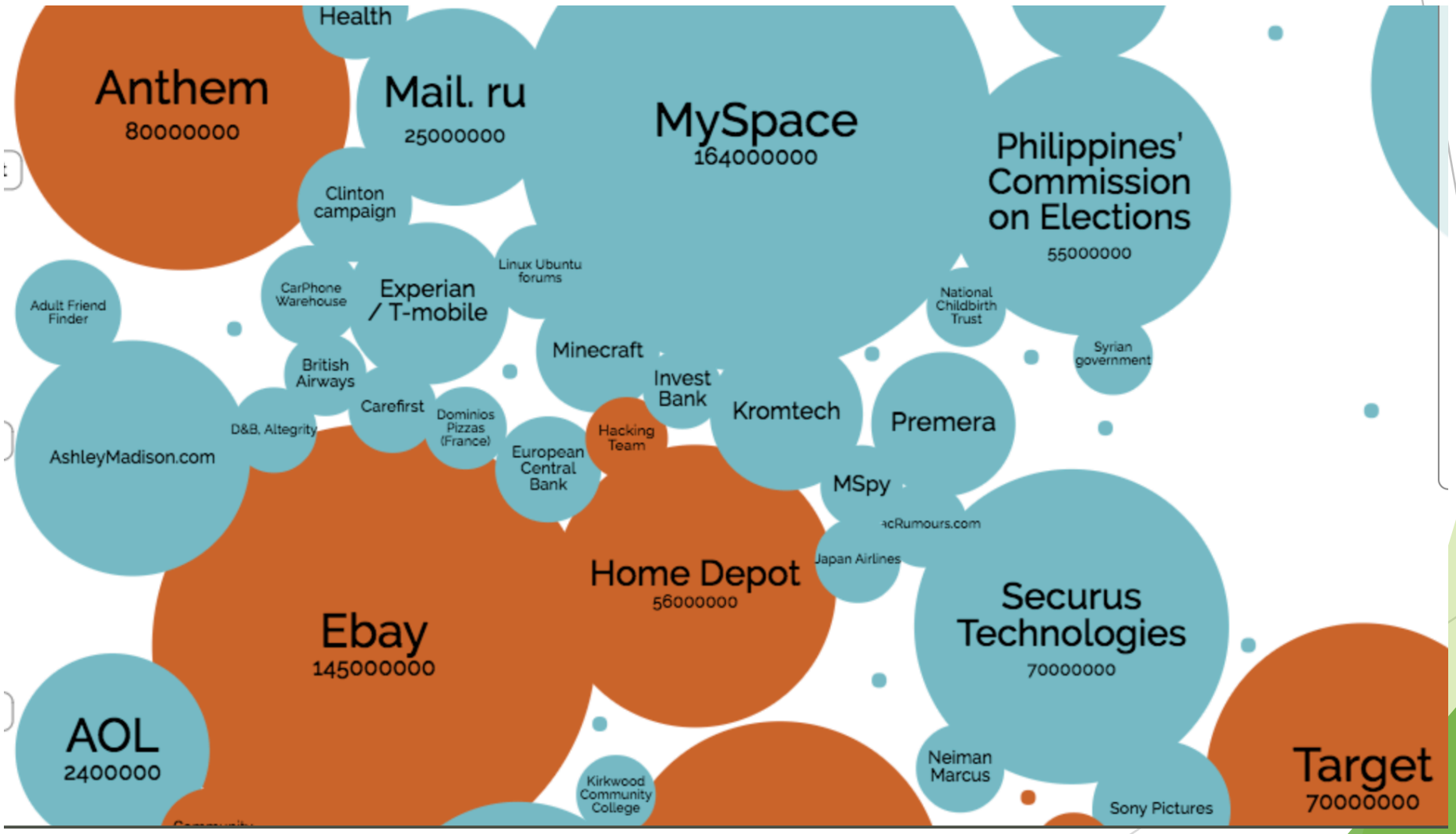
NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.



NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

Why do we care about cybersecurity?



NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

Who's on the receiving end of attacks?

Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	370	109	23	238
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

Table 1.

Number of security incidents by victim industry and organization size, 2015 dataset.

Source: Verizon 2016 Data Breach Investigations Report

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Why do attackers attack?

When poll is active, respond at **PollEv.com/cybersecure** Text **CYBERSECURE** to **22333** once to join

Why are these people attacking me?

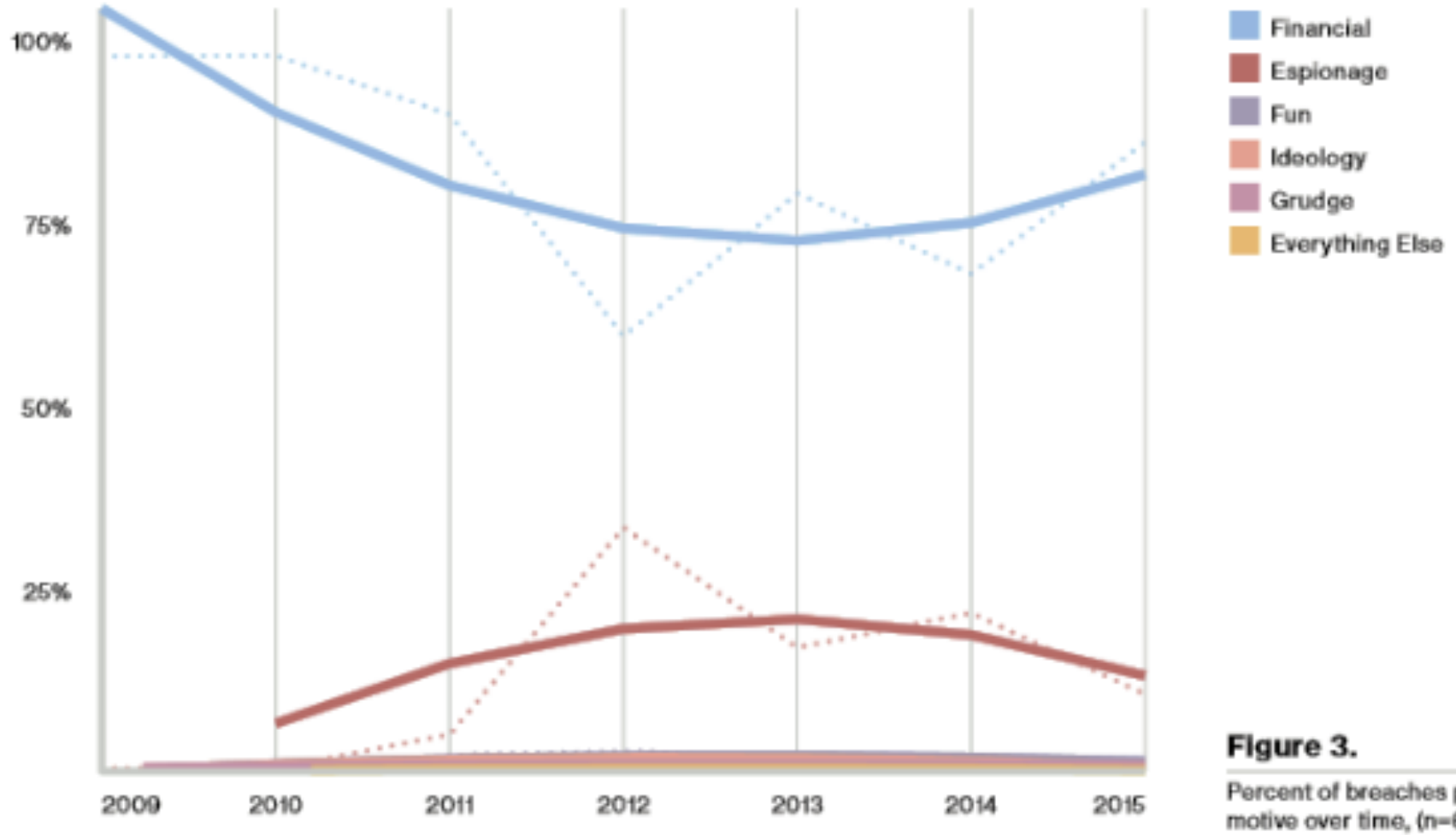


Figure 3.

Percent of breaches per threat actor motive over time, (n=6,762)

Source: Verizon 2016 Data Breach Investigations Report

NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

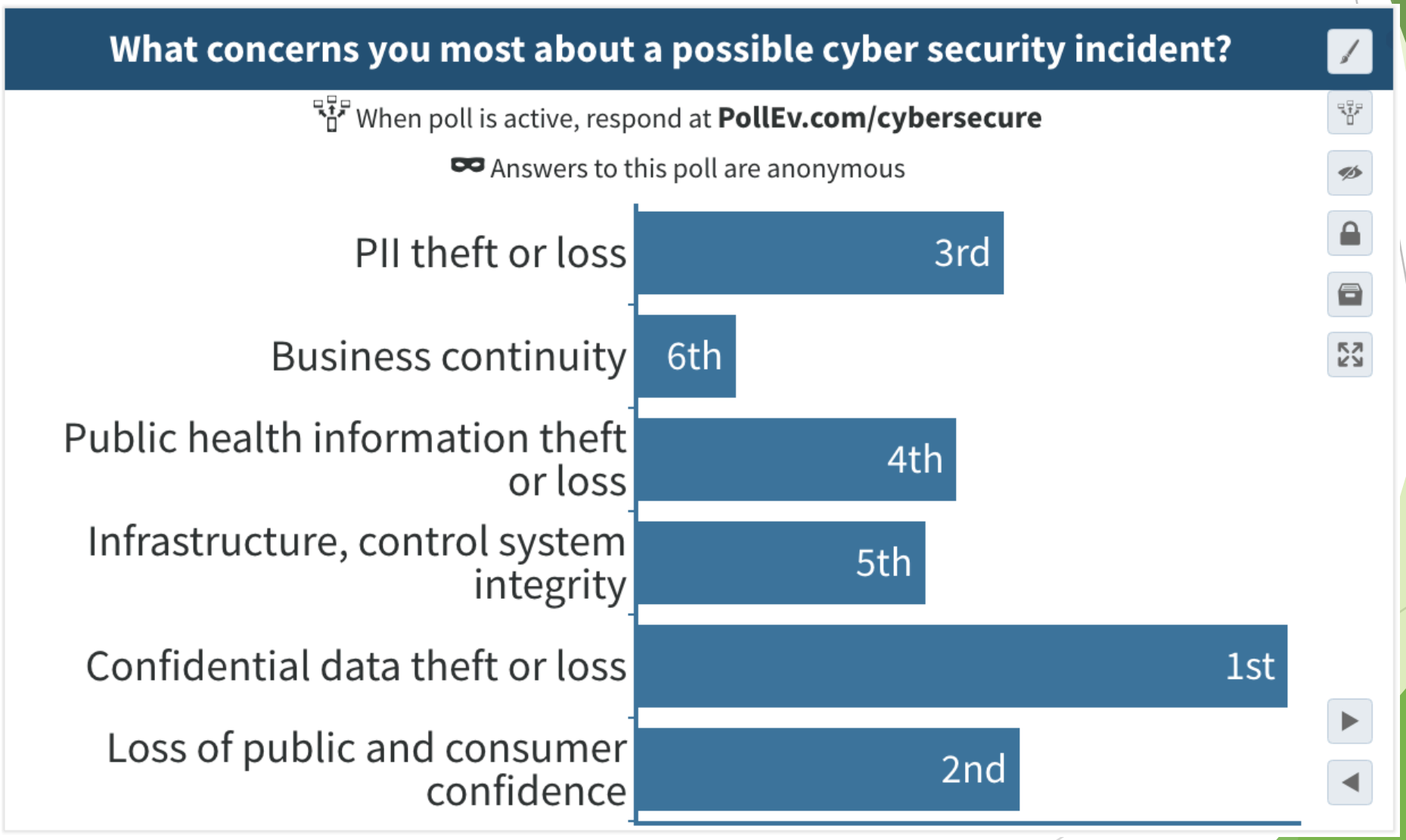
Why are these people attacking me?

89%

of breaches had a financial or espionage motive

Source: Verizon 2016 Data Breach Investigations Report

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.



NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

What is the cost of a data breach?

What concerns you most about advanced targeted attacks?

Confidential data theft	25%
Business continuity	20%
PII theft	17%
Loss of public and consumer confidence	16%
Infrastructure, control system integrity	9%
Public health information theft	5%

Source: Center for Digital Government 2014 Advanced Cyber Threats in State and Local Government

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

What is the cost of a data breach?

What do you think the impact of a serious breach could be to your organization?

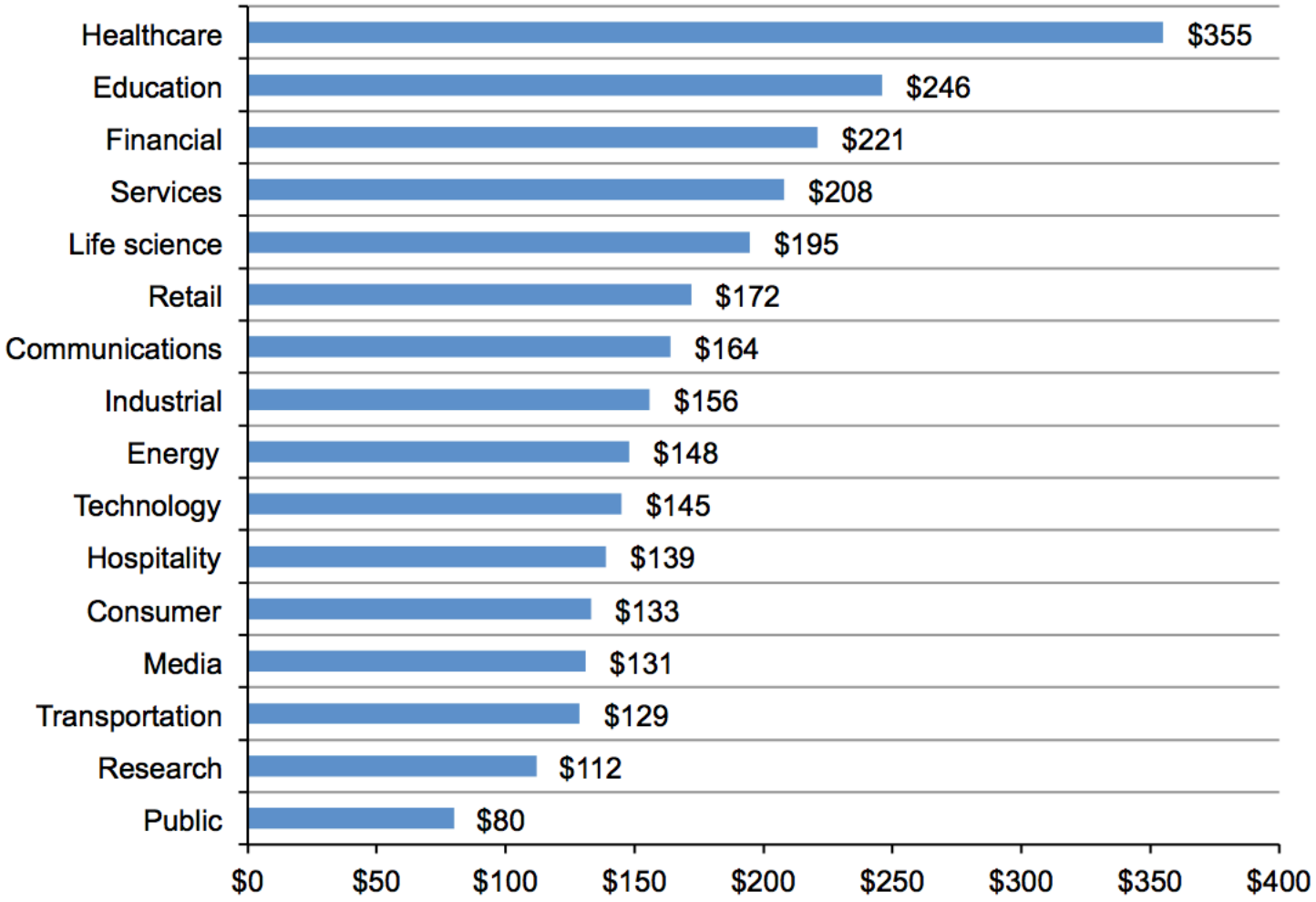
Less than $50,000	18%
$50,000	13%
$5 million	18%
$25 million	13%
Don't know	41%

Source: Center for Digital Government 2014 Advanced Cyber Threats in State and Local Government

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

What is the cost of a data breach?

Figure 4. Per capita cost by industry classification
Consolidated view (n=383), measured in US$



Source: Ponemon Institute 2016 Cost of Data Breach Study

NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

Why are these people attacking me?

Top 10 Types of Information Exposed

- *Financial information includes stolen credit card details and other financial credentials.*

	2015 Type	2015 %	2014 Type	2014 %
1	Real Names	78%	Real Names	69%
2	Home Addresses	44%	Gov. ID Numbers (e.g., SSN)	45%
3	Birth Dates	41%	Home Addresses	43%
4	Gov. ID Numbers (e.g., SSN)	38%	Financial Information	36%
5	Medical Records	36%	Birth Dates	35%
6	Financial Information	33%	Medical Records	34%
7	Email Addresses	21%	Phone Numbers	21%
8	Phone Numbers	19%	Email Addresses	20%
9	Insurance	13%	User Names & Passwords	13%
10	User Names & Passwords	11%	Insurance	11%

Source: Symantec 2016 Internet Security Threat Report

What methods are they using to attack me?

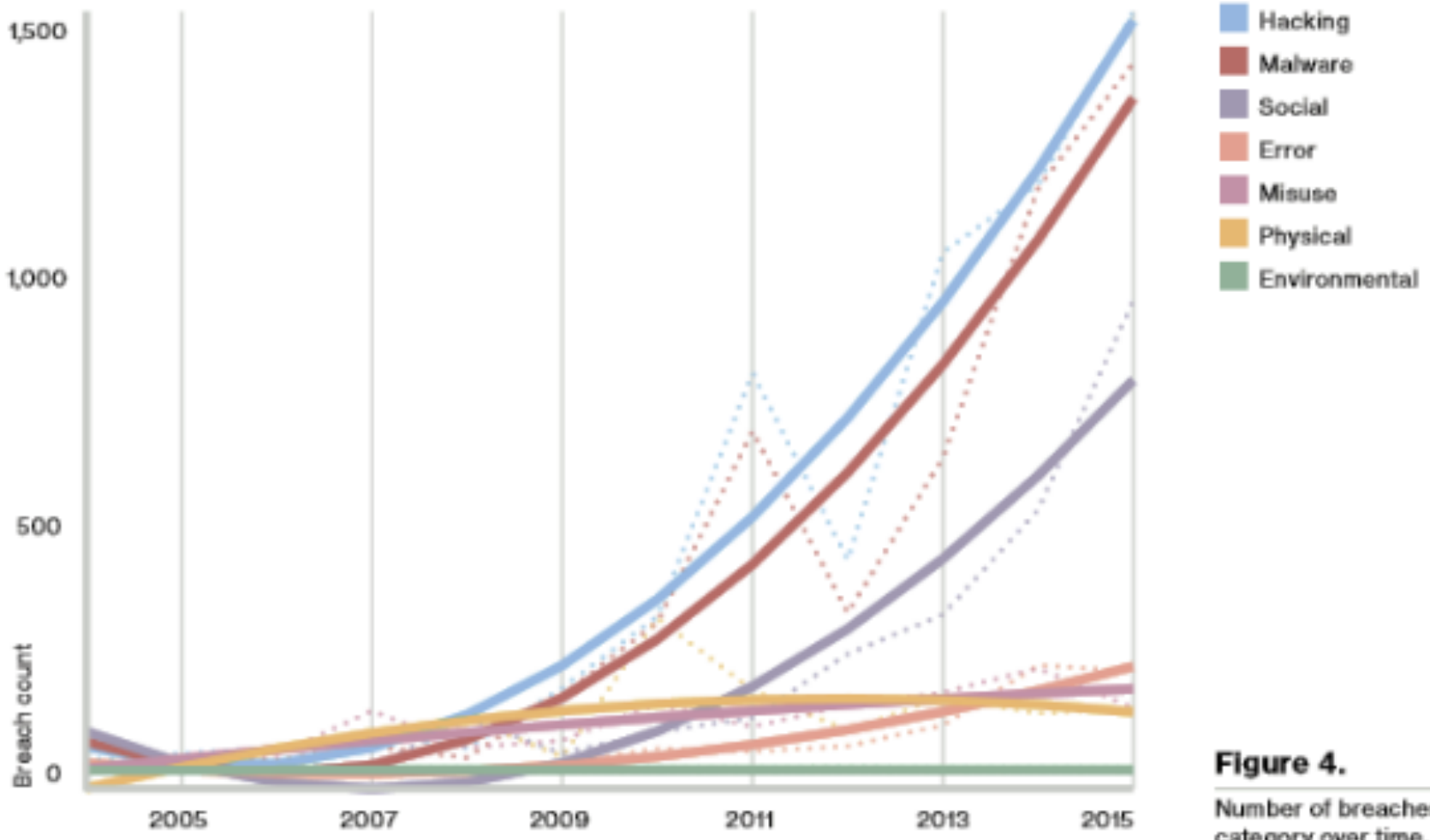


Figure 4.

Number of breaches per threat action category over time, (n=9,009)

Source: Verizon 2016 Data Breach Investigations Report

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Hacking

NORSE

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Hacking

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Malware

390,000 malicious programs are registered every day (AV-TEST, 2016)

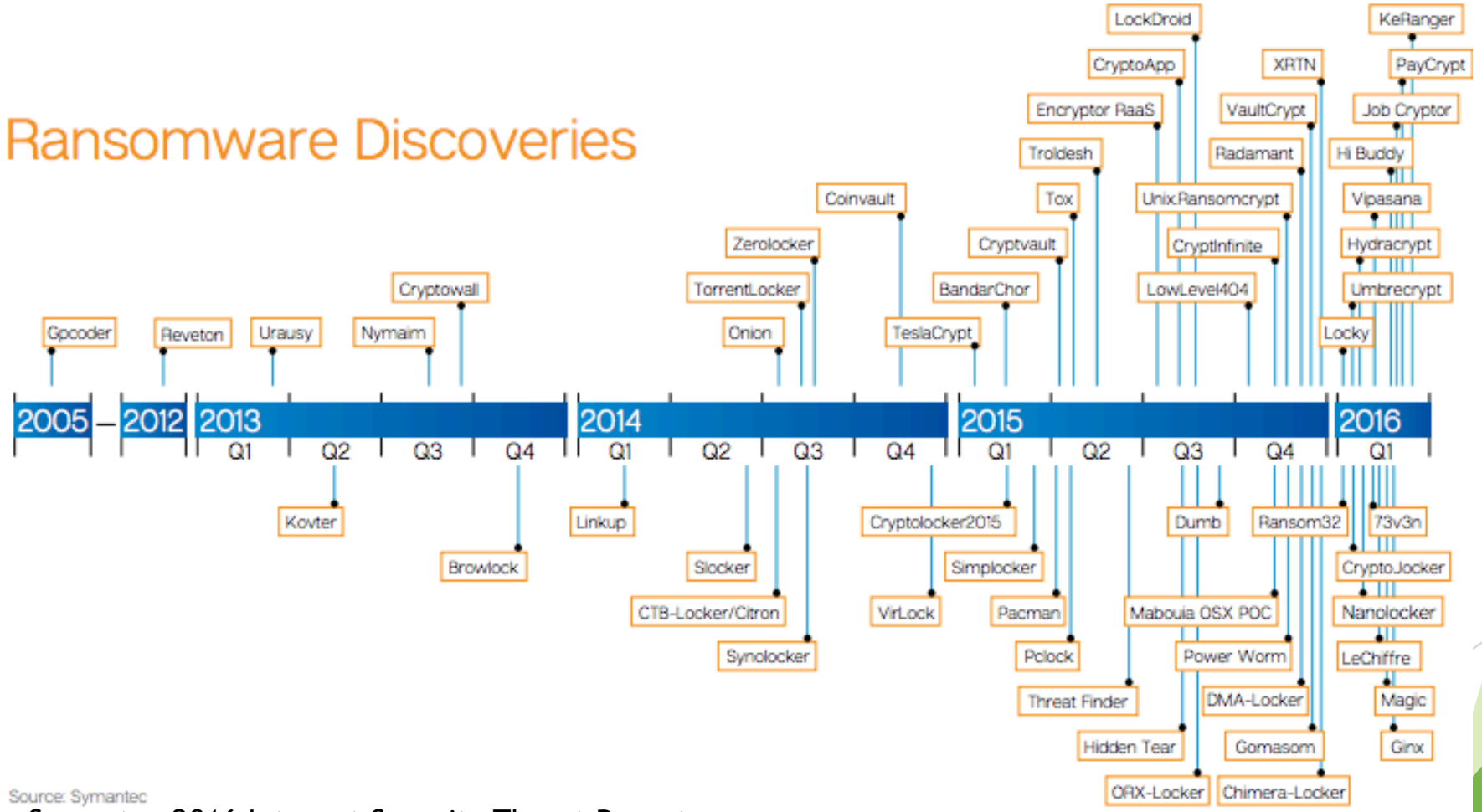
NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Malware

2,500 cases of ransomware costing victims $24 million in the US alone were reported to the Internet Crime Complaint Center for 2015 (Turkel, 2016)

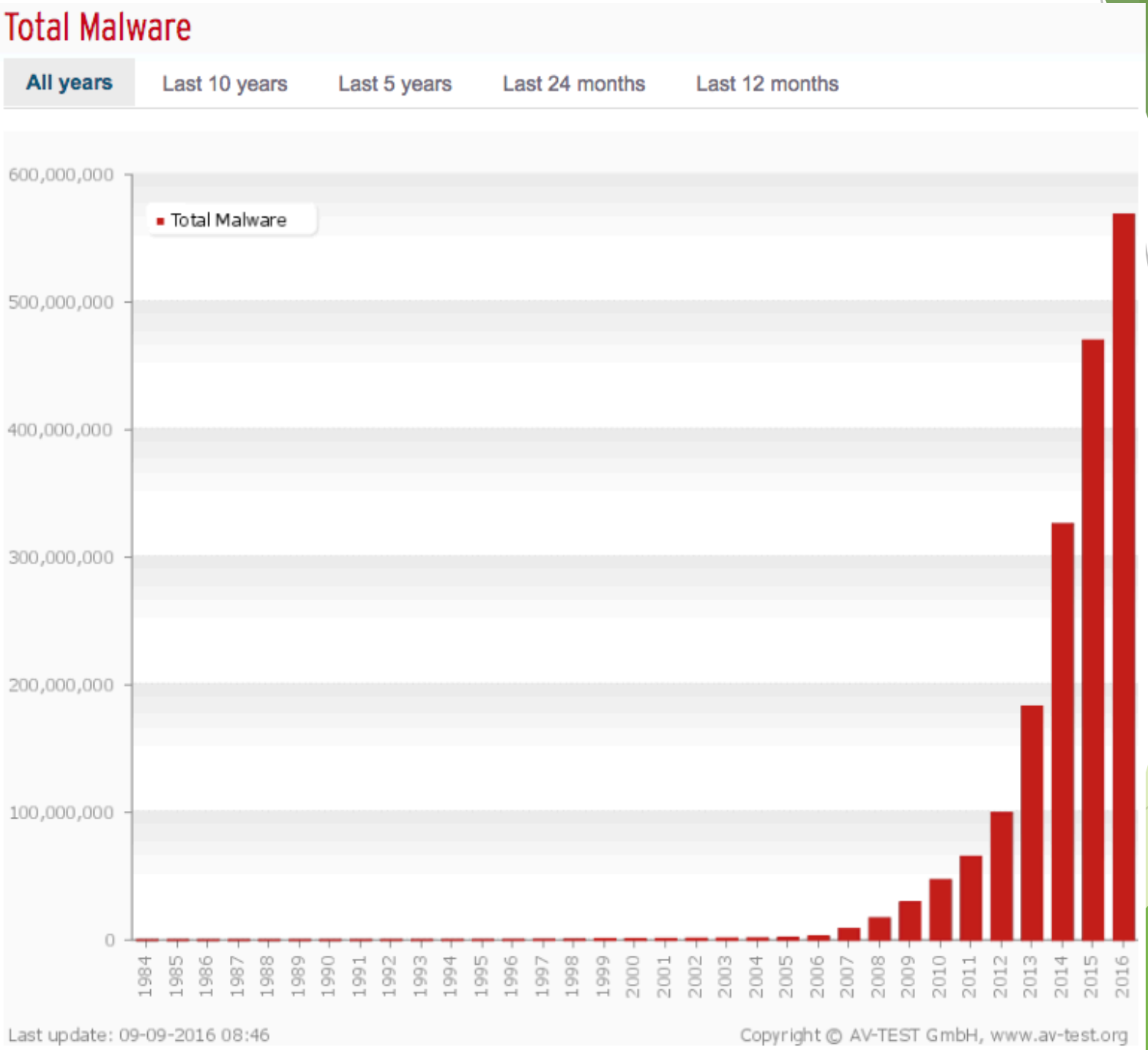
NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Malware



Source: Symantec 2016 Internet Security Threat Report

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.



NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

Social Attacks - Phishing

From: IRS Online <ahr@irxt.com>
Reply-To: "noreply@irxt.com" <noreply@irxt.com>
Date: Thursday, April 11, 2013 12:15 PM
Subject: Final reminder: Notice of Tax Return. ID: I3H583326/13

IRS

Department of the Treasury
Internal Revenue Service

04/11/2013

Referance: I3H583326/13

Claim Your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to $ 319.95.

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started

NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

Social Attacks - Phishing

From: on behalf of 05/01/2014 7:55 PM

Amazon <management@mazoncanada.ca>

not an Amazon email address (note the missing A in Amazon)

To: @sheridanc.on.ca

Cc:

Subject: Suspension

amazon.com

Dear Client,

Generic non-personalized greeting

We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else.In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it.

To confirm your identity with us click the link bellow:

https://www.amazon.com/exec/obidos/sign-in.html

Hovering over the link reveals it points to a non-Amazon site - "http://redirect.kereskedj.com"

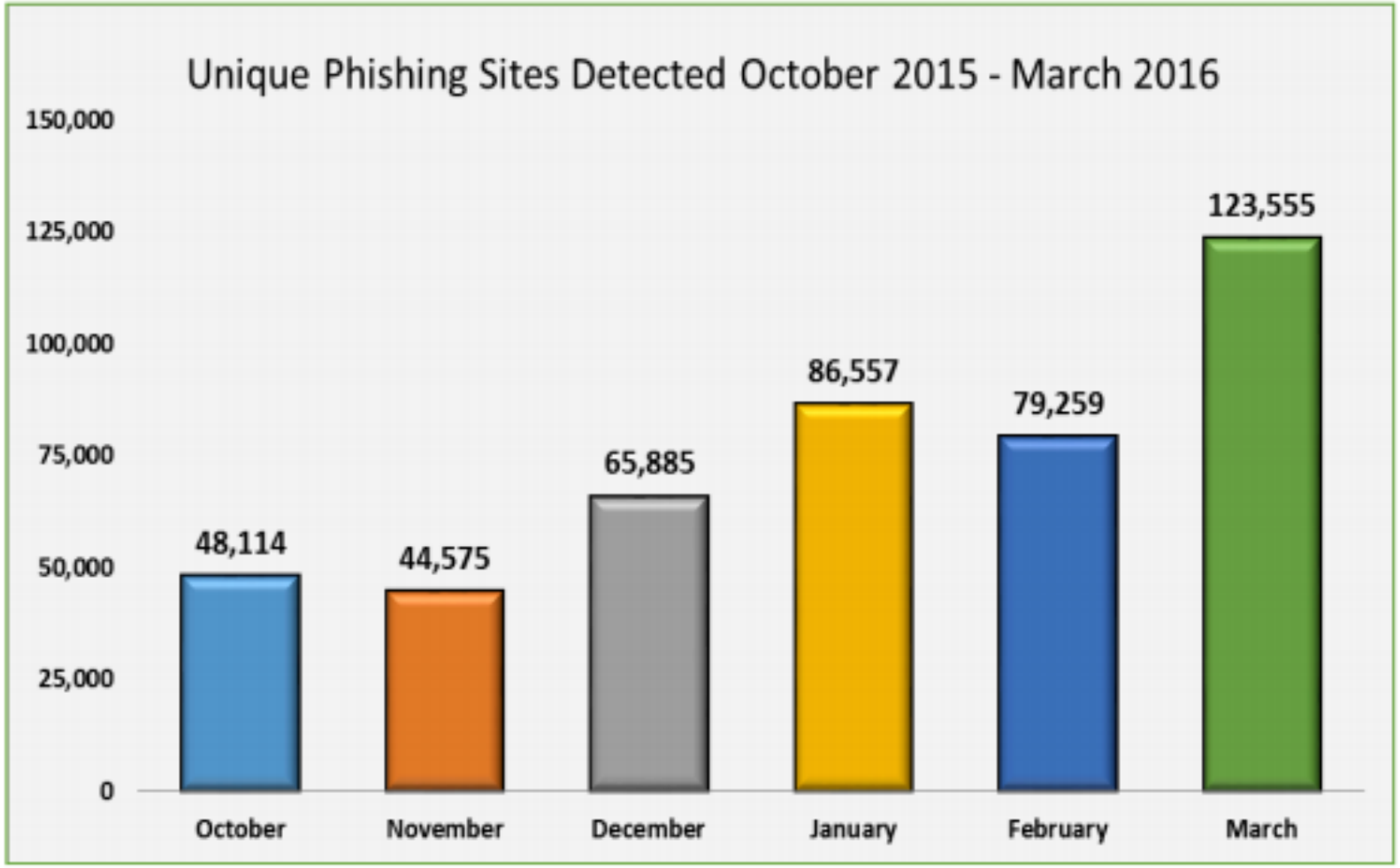
Sincerely,

The Amazon Associates Team

© 1996-2013, Amazon.com, Inc. or its affiliates

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Social Attacks - Phishing

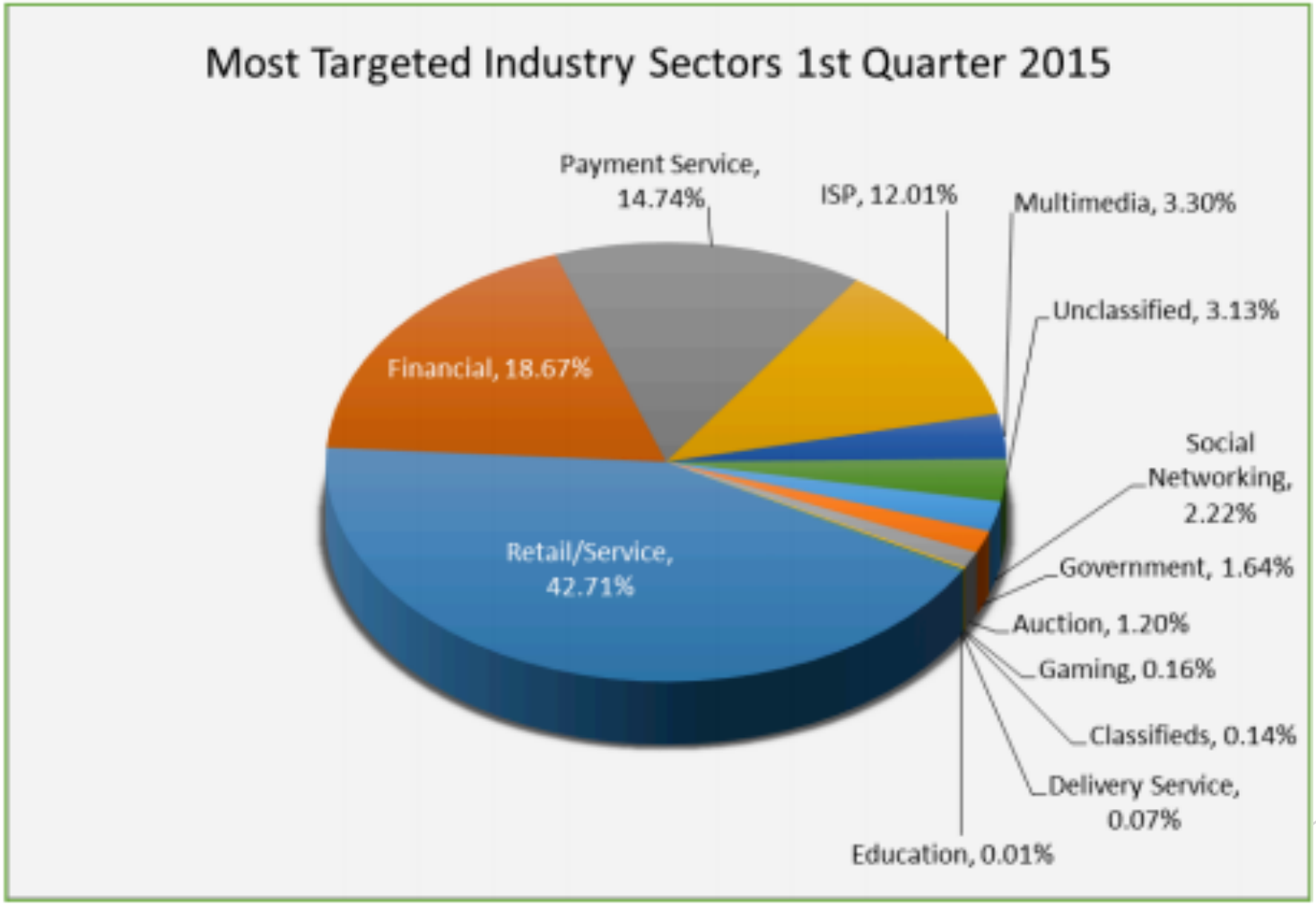


Source: Anti Phishing Working Group Activity Trends Report – May 23, 2016

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Social Attacks - Phishing



Source: Anti Phishing Working Group Activity Trends Report – May 23, 2016

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Social Attacks - Phishing

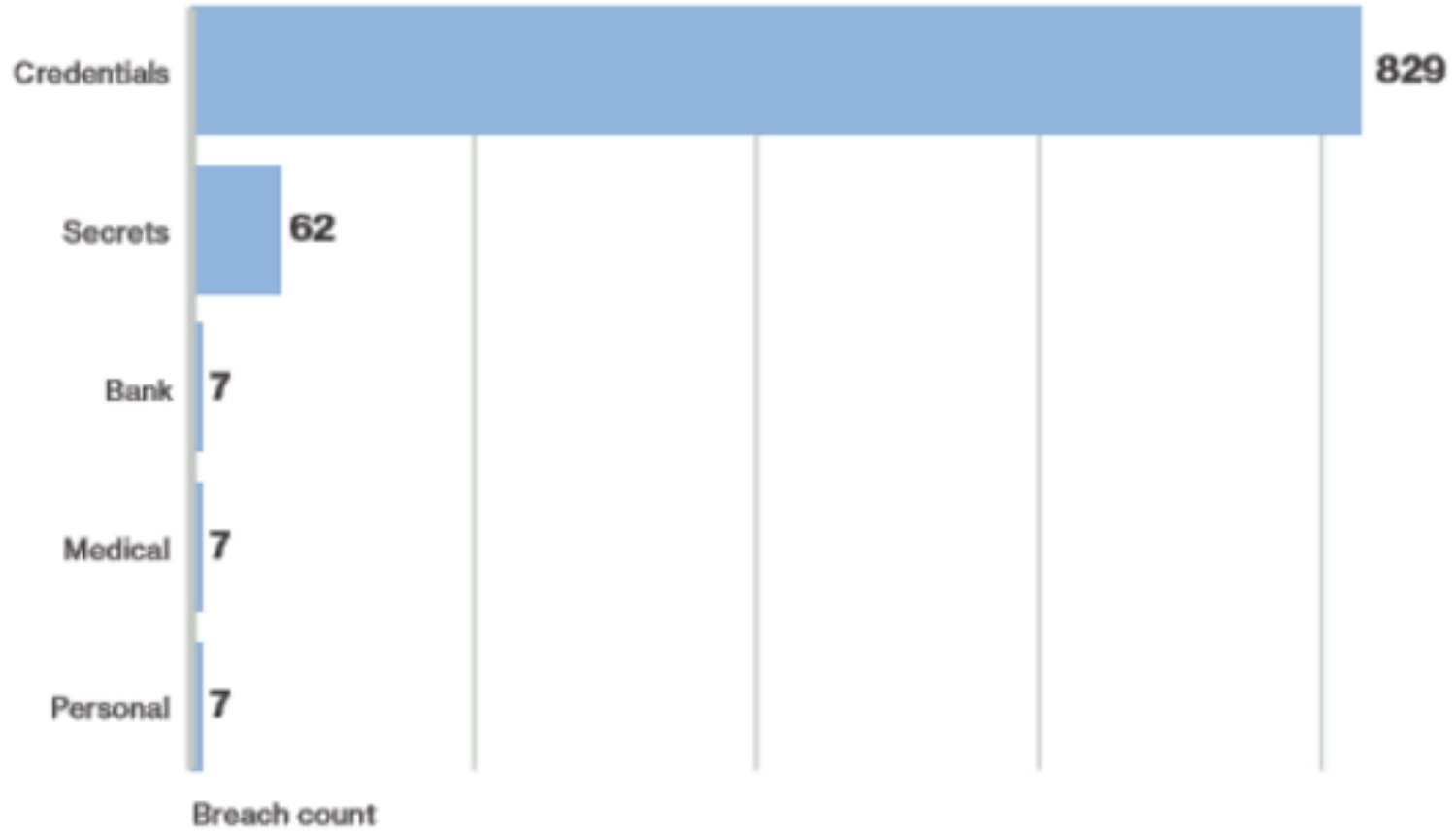


Figure 15.

Top five data varieties breached by phishing attacks, (n=905)

Source: Verizon 2016 Data Breach Investigations Report

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

What can we do about all of this?

NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

Ensure All Devices Allowed on Company Networks Have Adequate Security Protections

If a bring-your-own-device (BYOD) policy is in place, ensure a minimal security profile is established for any devices that are allowed access to the network.

Implement a Removable Media Policy

Where practical, restrict unauthorized devices, such as external portable hard-drives and other removable media. Such devices can both introduce malware and facilitate intellectual property breaches, whether intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

Be Aggressive in Updating and Patching

Update, patch, and migrate from outdated and insecure browsers, applications, and browser plugins. This also applies to operating systems, not just across computers, but mobile, ICS, and IoT devices as well. Keep virus and intrusion prevention definitions at the latest available versions using vendors' automatic updates.

Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

Enforce an Effective Password Policy

Ensure passwords are strong. Passwords should be at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple websites and sharing passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days.

Ensure Regular Backups Are Available

Create and maintain regular backups of critical systems, as well as endpoints. In the event of a security or data emergency, backups should be easily accessible to minimize downtime of services and employee productivity.

Restrict Email Attachments

Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments. Ensure that mail servers are adequately protected by security software and that email is thoroughly scanned.

Ensure Infection and Incident Response Procedures Are in Place

- Keep your security vendor contact information handy; know who you will call, and what steps you will take if you have one or more infected systems.
- Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss.
- Make use of post-infection detection capabilities from web gateway, endpoint security solutions and firewalls to identify infected systems.
- Isolate infected computers to prevent the risk of further infection within the organization, and restore using trusted backup media.
- If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied.

Educate Employees

As ever, basic common sense and the introduction of good security habits can go a long way to keeping sites and servers safe this year.

- Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless from a trusted source or the download has been scanned for malware.
- Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends.
- Deploy web browser URL reputation plugin solutions that display the reputation of websites from searches.
- Restrict software to corporate-approved applications, if possible, and avoid downloading software from file sharing sites. Only download packages directly from trusted vendors' websites.

Source: Symantec 2016 Internet Security Threat Report

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

- Educate users on safe social media conduct. Offers that look too good usually are, and hot topics are prime bait for scams. Not all links lead to real login pages.
- Encourage them to adopt two-step authentication on any website or app that offers it.
- Ensure they have different passwords for every email account, applications and login—especially for work-related sites and services.
- Remind then to use common sense. Having antivirus and security software doesn't mean it is ok to visit malicious or questionable websites.
- Encourage employees to raise the alarm if they see anything suspicious. For example, if Windows users see a warning indicating that they are "infected" after clicking on a URL or using a search engine (indicative of fake antivirus infections), educate users to close or quit the browser using Alt-F4, CTRL+W or to use the task manager, and then notify the helpdesk.

Protect Mobile Devices

We recommend that people and employers treat mobile devices like the small, powerful computers that they are and protect them accordingly using:

- Access control, including biometrics where possible.
- Data loss prevention, such as on-device encryption.
- Automated device backup.
- Remote find and wipe.
- Regular updating. For example, the latest version of Android, codenamed 'Honeycomb', includes a number of features designed specifically to thwart attackers.
- Common sense. Don't jailbreak devices and only use trusted app markets.
- Training, particularly around paying attention to permissions requested by an app.
- Security solutions such as Symantec Mobility or Norton Mobile Security

We have seen the number of mobile vulnerabilities increase every year over the past three years—although this is perhaps an indicator of progress rather than a cause for despair. It is an indication that security researchers, operating system developers and app writers are, in fact, paying more attention to mobile security by identifying and fixing more problems.

Although we expect mobile devices to come under growing attack over the next year, there is also hope that with the right preventative measures and continuing investment in security, users can achieve a high level of protection against them.

Building Security into Devices

The diverse nature of ICS and IoT platforms make host-based intrusion detection systems (IDS) and intrusion prevention systems (IPS), with customizable rulesets and policies that are unique to a platform and application, suitable solutions.

However, manufacturers of ICS and IoT devices are largely responsible for ensuring that security is built into the devices before shipping.

Building security directly into the software and applications that run on the ICS and IoT devices should prevent many attacks that manage to side-step defenses at the upper layers. Manufacturers should adopt and integrate such principles into their software development processes.

Business users and consumers need to be assured that suppliers are fundamentally building security into the IoT devices that they are buying, rather than it being considered as a bolt-on option.

It's a Team Effort

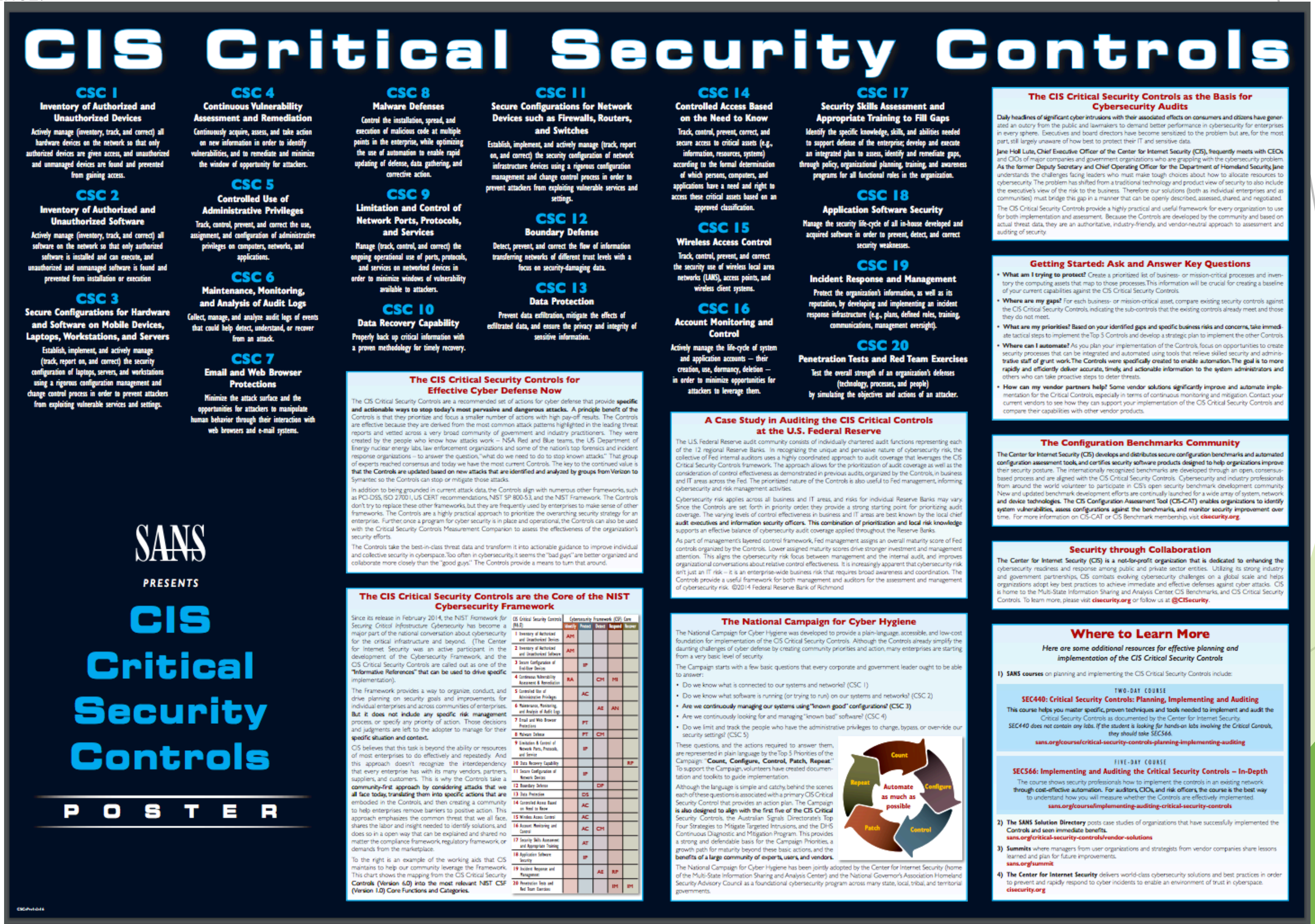
Consumer confidence is built up over multiple interactions across numerous websites owned by countless different organizations. But it only takes one bad experience of stolen data or a drive-by download to tarnish the reputation of every website in the consumer's mind.

As we said at the start of the report, there is a real opportunity in the coming year to reduce the number of successful web attacks and limit the risks websites potentially pose to consumers, but it will take commitment and action from website owners for it to become a reality.

Adopt Complete Website Security in 2016, and together with Symantec, make it a good year for cybersecurity and a very bad one for cybercriminals. ■

NORTH DAKOTA
UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.



CIS Critical Security Controls

CSC 1
Inventory of Authorized and Unauthorized Devices
Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

CSC 2
Inventory of Authorized and Unauthorized Software
Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution

CSC 3
Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
Establish, implement, and actively manage (track, report on, and correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 4
Continuous Vulnerability Assessment and Remediation
Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, and to remediate and minimize the window of opportunity for attackers.

CSC 5
Controlled Use of Administrative Privileges
Track, control, prevent, and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

CSC 6
Maintenance, Monitoring, and Analysis of Audit Logs
Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

CSC 7
Email and Web Browser Protections
Minimize the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems.

CSC 8
Malware Defenses
Control the installation, spread, and execution of malicious code at multiple points in the enterprise, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.

CSC 9
Limitation and Control of Network Ports, Protocols, and Services
Manage (track, control, and correct) the ongoing operational use of ports, protocols, and services on networked devices in order to minimize windows of vulnerability available to attackers.

CSC 10
Data Recovery Capability
Properly back up critical information with a proven methodology for timely recovery.

CSC 11
Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
Establish, implement, and actively manage (track, report on, and correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.

CSC 12
Boundary Defense
Detect, prevent, and correct the flow of information transferring networks of different trust levels with a focus on security-damaging data.

CSC 13
Data Protection
Prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

CSC 14
Controlled Access Based on the Need to Know
Track, control, prevent, correct, and secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.

CSC 15
Wireless Access Control
Track, control, prevent, and correct the security use of wireless local area networks (LANS), access points, and wireless client systems.

CSC 16
Account Monitoring and Control
Actively manage the life-cycle of system and application accounts – their creation, use, dormancy, deletion – in order to minimize opportunities for attackers to leverage them.

CSC 17
Security Skills Assessment and Appropriate Training to Fill Gaps
Identify the specific knowledge, skills, and abilities needed to support defense of the enterprise; develop and execute an integrated plan to assess, identify and remediate gaps, through policy, organizational planning, training, and awareness programs for all functional roles in the organization.

CSC 18
Application Software Security
Manage the security life-cycle of all in-house developed and acquired software in order to prevent, detect, and correct security weaknesses.

CSC 19
Incident Response and Management
Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure (e.g., plans, defined roles, training, communications, management oversight).

CSC 20
Penetration Tests and Red Team Exercises
Test the overall strength of an organization's defenses (technology, processes, and people) by simulating the objectives and actions of an attacker.

SANS
PRESENTS
CIS Critical Security Controls
POSTER

The CIS Critical Security Controls for Effective Cyber Defense Now

The CIS Critical Security Controls are a recommended set of actions for cyber defense that provide **specific and actionable ways to stop today's most pervasive and dangerous attacks.** A principle benefit of the Controls is that they prioritize and focus a smaller number of actions with high pay-off results. The Controls are effective because they are derived from the most common attack patterns highlighted in the leading threat reports and vetted across a very broad community of government and industry practitioners. They were created by the people who know how attacks work – NSA Red and Blue teams, the US Department of Energy nuclear energy labs, law enforcement organizations and some of the nation's top forensics and incident response organizations – to answer the question, "what do we need to do to stop known attacks." That group of experts reached consensus and today we have the most current Controls. The key to the continued value is **that the Controls are updated based on new attacks that are identified and analyzed by groups from Verizon to** Symantec so the Controls can stop or mitigate those attacks.

In addition to being grounded in current attack data, the Controls align with numerous other frameworks, such as PCI-DSS, ISO 27001, US CERT recommendations, NIST SP 800-53, and the NIST Framework. The Controls don't try to replace these other frameworks, but they are frequently used by enterprises to make sense of other frameworks. The Controls are a highly practical approach to prioritize the overarching security strategy for an enterprise. Further, once a program for cyber security is in place and operational, the Controls can also be used with the Critical Security Controls Measurement Companion to assess the effectiveness of the organization's security efforts.

The Controls take the best-in-class threat data and transform it into actionable guidance to improve individual and collective security in cyberspace. Too often in cybersecurity, it seems the "bad guys" are better organized and collaborate more closely than the "good guys." The Controls provide a means to turn that around.

The CIS Critical Security Controls are the Core of the NIST Cybersecurity Framework

Since its release in February 2014, the NIST *Framework for Securing Critical Infrastructure Cybersecurity* has become a major part of the national conversation about cybersecurity for the critical infrastructure and beyond. (The Center for Internet Security was an active participant in the development of the Cybersecurity Framework, and the CIS Critical Security Controls are called out as one of the **"Informative References" that can be used to drive specific** implementation).

The Framework provides a way to organize, conduct, and drive planning on security goals and improvements, for individual enterprises and across communities of enterprises. **But it does not include any specific risk management** process, or specify any priority of action. Those decisions and judgments are left to the adopter to manage for their **specific situation and context.**

CIS believes that this task is beyond the ability or resources of most enterprises to do effectively and repeatedly. And this approach doesn't recognize the interdependency that every enterprise has with its many vendors, partners, suppliers, and customers. This is why the Controls take a **community-first approach by considering attacks that we all face today, translating them into specific actions that are** embodied in the Controls, and then creating a community to help enterprises remove barriers to positive action. This approach emphasizes the common threat that we all face, shares the labor and insight needed to identify solutions, and does so in a open way that can be explained and shared no matter the compliance framework, regulatory framework, or demands from the marketplace.

To the right is an example of the working aids that CIS maintains to help our community leverage the Framework. This chart shows the mapping from the CIS Critical Security **Controls (Version 6.0) into the most relevant NIST CSF (Version 1.0) Core Functions and Categories.**

CIS Critical Security Controls (V6.0)	Cybersecurity Framework (CSF) Core: Identify	Protect	Detect	Respond	Recover
1 Inventory of Authorized and Unauthorized Devices	AM				
2 Inventory of Authorized and Unauthorized Software	AM				
3 Secure Configuration of End-User Devices		IP			
4 Continuous Vulnerability Assessment & Remediation	RA		CM	MI	
5 Controlled Use of Administrative Privileges		AC			
6 Maintenance, Monitoring, and Analysis of Audit Logs			AE	AN	
7 Email and Web Browser Protections		PT			
8 Malware Defense		PT	CM		
9 Limitation & Control of Network Ports, Protocols, and Service		IP			
10 Data Recovery Capability					RP
11 Secure Configuration of Network Devices		IP			
12 Boundary Defense			DP		
13 Data Protection		DS			
14 Controlled Access Based on Need to Know		AC			
15 Wireless Access Control		AC			
16 Account Monitoring and Control		AC	CM		
17 Security Skills Assessment and Appropriate Training		AT			
18 Application Software Security		IP			
19 Incident Response and Management			AE	RP	
20 Penetration Tests and Red Team Exercises				IM	IM

A Case Study in Auditing the CIS Critical Controls at the U.S. Federal Reserve

The U.S. Federal Reserve audit community consists of individually chartered audit functions representing each of the 12 regional Reserve Banks. In recognizing the unique and pervasive nature of cybersecurity risk, the collective of Fed internal auditors uses a highly coordinated approach to audit coverage that leverages the CIS Critical Security Controls framework. The approach allows for the prioritization of audit coverage as well as the consideration of control effectiveness as demonstrated in previous audits, organized by the Controls, in business and IT areas across the Fed. The prioritized nature of the Controls is also useful to Fed management, informing cybersecurity and risk management activities.

Cybersecurity risk applies across all business and IT areas, and risks for individual Reserve Banks may vary. Since the Controls are set forth in priority order, they provide a strong starting point for prioritizing audit coverage. The varying levels of control effectiveness in business and IT areas are best known by the local chief **audit executives and information security officers. This combination of prioritization and local risk knowledge** supports an effective balance of cybersecurity audit coverage applied throughout the Reserve Banks.

As part of management's layered control framework, Fed management assigns an overall maturity score of Fed controls organized by the Controls. Lower assigned maturity scores drive stronger investment and management attention. This aligns the cybersecurity risk focus between management and the internal audit, and improves organizational conversations about relative control effectiveness. It is increasingly apparent that cybersecurity risk isn't just an IT risk – it is an enterprise-wide business risk that requires broad awareness and coordination. The Controls provide a useful framework for both management and auditors for the assessment and management of cybersecurity risk. ©2014 Federal Reserve Bank of Richmond

The National Campaign for Cyber Hygiene

The National Campaign for Cyber Hygiene was developed to provide a plain-language, accessible, and low-cost foundation for implementation of the CIS Critical Security Controls. Although the Controls already simplify the daunting challenges of cyber defense by creating community priorities and action, many enterprises are starting from a very basic level of security.

The Campaign starts with a few basic questions that every corporate and government leader ought to be able to answer:

- Do we know what is connected to our systems and networks? (CSC 1)
- Do we know what software is running (or trying to run) on our systems and networks? (CSC 2)
- **Are we continuously managing our systems using "known good" configurations? (CSC 3)**
- Are we continuously looking for and managing "known bad" software? (CSC 4)
- Do we limit and track the people who have the administrative privileges to change, bypass, or over-ride our security settings? (CSC 5)

These questions, and the actions required to answer them, are represented in plain language by the Top 5 Priorities of the Campaign: "**Count, Configure, Control, Patch, Repeat.**" To support the Campaign, volunteers have created documentation and toolkits to guide implementation.

Although the language is simple and catchy, behind the scenes each of these questions is associated with a primary CIS Critical Security Control that provides an action plan. The Campaign **is also designed to align with the first five of the CIS Critical** Security Controls, the Australian Signals Directorate's Top Four Strategies to Mitigate Targeted Intrusions, and the DHS Continuous Diagnostic and Mitigation Program. This provides a strong and defendable basis for the Campaign Priorities, a growth path for maturity beyond these basic actions, and the **benefits of a large community of experts, users, and vendors.**

The National Campaign for Cyber Hygiene has been jointly adopted by the Center for Internet Security (home of the Multi-State Information Sharing and Analysis Center) and the National Governor's Association Homeland Security Advisory Council as a foundational cybersecurity program across many state, local, tribal, and territorial governments.

The CIS Critical Security Controls as the Basis for Cybersecurity Audits

Daily headlines of significant cyber intrusions with their associated effects on consumers and citizens have gener-ated an outcry from the public and lawmakers to demand better performance in cybersecurity for enterprises in every sphere. Executives and board directors have become sensitized to the problem but are, for the most part, still largely unaware of how best to protect their IT and sensitive data.

Jane Holl Lute, Chief Executive Officer of the Center for Internet Security (CIS), frequently meets with CEOs and CIOs of major companies and government organizations who are grappling with the cybersecurity problem. **As the former Deputy Secretary and Chief Operating Officer for the Department of Homeland Security, Jane** understands the challenges facing leaders who must make tough choices about how to allocate resources to cybersecurity. The problem has shifted from a traditional technology and product view of security to also include the executive's view of the risk to the business. Therefore our solutions (both as individual enterprises and as communities) must bridge this gap in a manner that can be openly described, assessed, shared, and negotiated.

The CIS Critical Security Controls provide a highly practical and useful framework for every organization to use for both implementation and assessment. Because the Controls are developed by the community and based on actual threat data, they are an authoritative, industry-friendly, and vendor-neutral approach to assessment and auditing of security.

Getting Started: Ask and Answer Key Questions

- **What am I trying to protect?** Create a prioritized list of business- or mission-critical processes and inventory the computing assets that map to those processes. This information will be crucial for creating a baseline of your current capabilities against the CIS Critical Security Controls.
- **Where are my gaps?** For each business- or mission-critical asset, compare existing security controls against the CIS Critical Security Controls, indicating the sub-controls that the existing controls already meet and those they do not meet.
- **What are my priorities? Based on your identified gaps and specific business risks and concerns, take immedi-**ate tactical steps to implement the Top 5 Controls and develop a strategic plan to implement the other Controls.
- **Where can I automate?** As you plan your implementation of the Controls, focus on opportunities to create security processes that can be integrated and automated using tools that relieve skilled security and adminis**trative staff of grunt work. The Controls were specifically created to enable automation. The goal is to more rapidly and efficiently deliver accurate, timely, and actionable information to the system administrators and** others who can take proactive steps to deter threats.
- **How can my vendor partners help? Some vendor solutions significantly improve and automate imple-**mentation for the Critical Controls, especially in terms of continuous monitoring and mitigation. Contact your current vendors to see how they can support your implementation of the CIS Critical Security Controls and compare their capabilities with other vendor products.

The Configuration Benchmarks Community

The Center for Internet Security (CIS) develops and distributes secure configuration benchmarks and automated configuration assessment tools, and certifies security software products designed to help organizations improve their security posture. The internationally recognized benchmarks are developed through an open, consensus-based process and are aligned with the CIS Critical Security Controls. Cybersecurity and industry professionals from around the world volunteer to participate in CIS's open security benchmark development community. New and updated benchmark development efforts are continually launched for a wide array of system, network **and device technologies. The CIS Configuration Assessment Tool (CIS-CAT) enables organizations to identify system vulnerabilities, assess configurations against the benchmarks, and monitor security improvement over** time. For more information on CIS-CAT or CIS Benchmark membership, visit **cisecurity.org**.

Security through Collaboration

The Center for Internet Security (CIS) is a not-for-profit organization that is dedicated to enhancing the cybersecurity readiness and response among public and private sector entities. Utilizing its strong industry and government partnerships, CIS combats evolving cybersecurity challenges on a global scale and helps organizations adopt key best practices to achieve immediate and effective defenses against cyber attacks. CIS is home to the Multi-State Information Sharing and Analysis Center, CIS Benchmarks, and CIS Critical Security Controls. To learn more, please visit **cisecurity.org** or follow us at **@CISecurity**.

Where to Learn More

Here are some additional resources for effective planning and implementation of the CIS Critical Security Controls

1) **SANS courses** on planning and implementing the CIS Critical Security Controls include:

TWO-DAY COURSE
SEC440: Critical Security Controls: Planning, Implementing and Auditing
This course helps you master specific, proven techniques and tools needed to implement and audit the Critical Security Controls as documented by the Center for Internet Security.
SEC440 does not contain any labs. If the student is looking for hands-on labs involving the Critical Controls, they should take SEC566.
sans.org/course/critical-security-controls-planning-implementing-auditing

FIVE-DAY COURSE
SEC566: Implementing and Auditing the Critical Security Controls – In-Depth
The course shows security professionals how to implement the controls in an existing network through cost-effective automation. For auditors, CIOs, and risk officers, the course is the best way to understand how you will measure whether the Controls are effectively implemented.
sans.org/course/implementing-auditing-critical-security-controls

2) **The SANS Solution Directory** posts case studies of organizations that have successfully implemented the Controls and seen immediate benefits.
sans.org/critical-security-controls/vendor-solutions

3) **Summits** where managers from user organizations and strategists from vendor companies share lessons learned and plan for future improvements.
sans.org/summit

4) **The Center for Internet Security** delivers world-class cybersecurity solutions and best practices in order to prevent and rapidly respond to cyber incidents to enable an environment of trust in cyberspace.
cisecurity.org

CSCsPoster2016

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

What can we do about all of this?

Let's focus on the top three methods of attack:

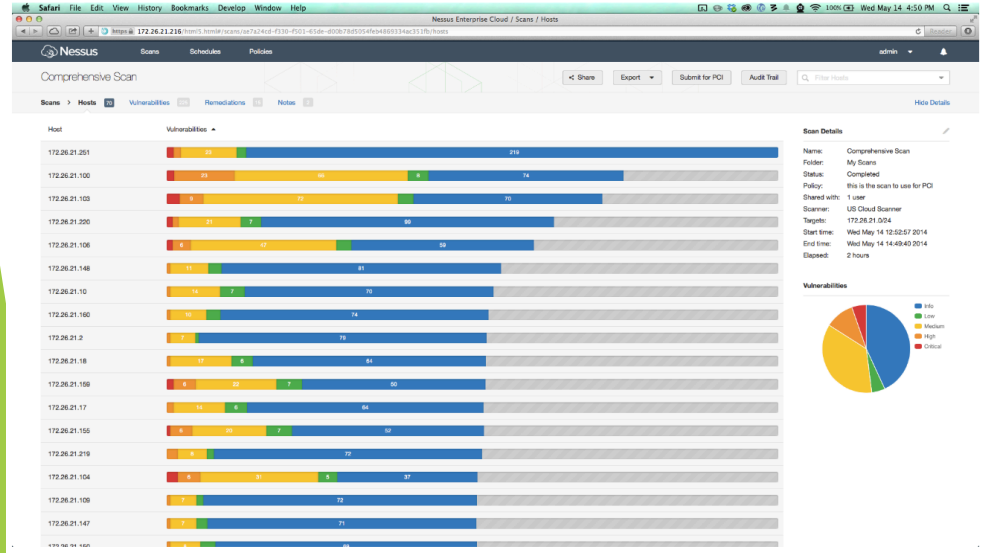
- Hacking
- Malware
- Social

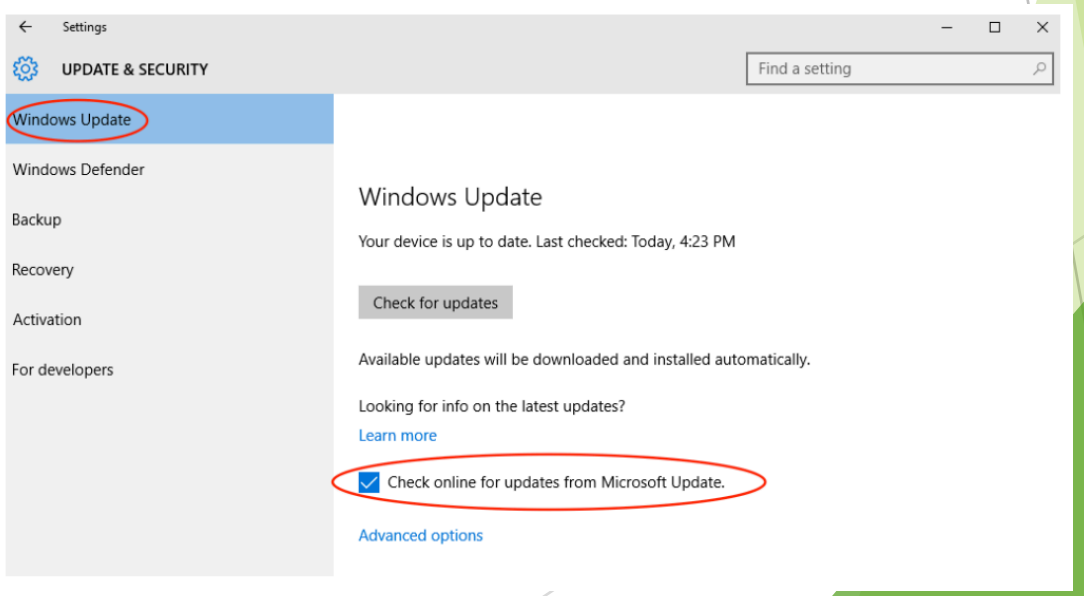
NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

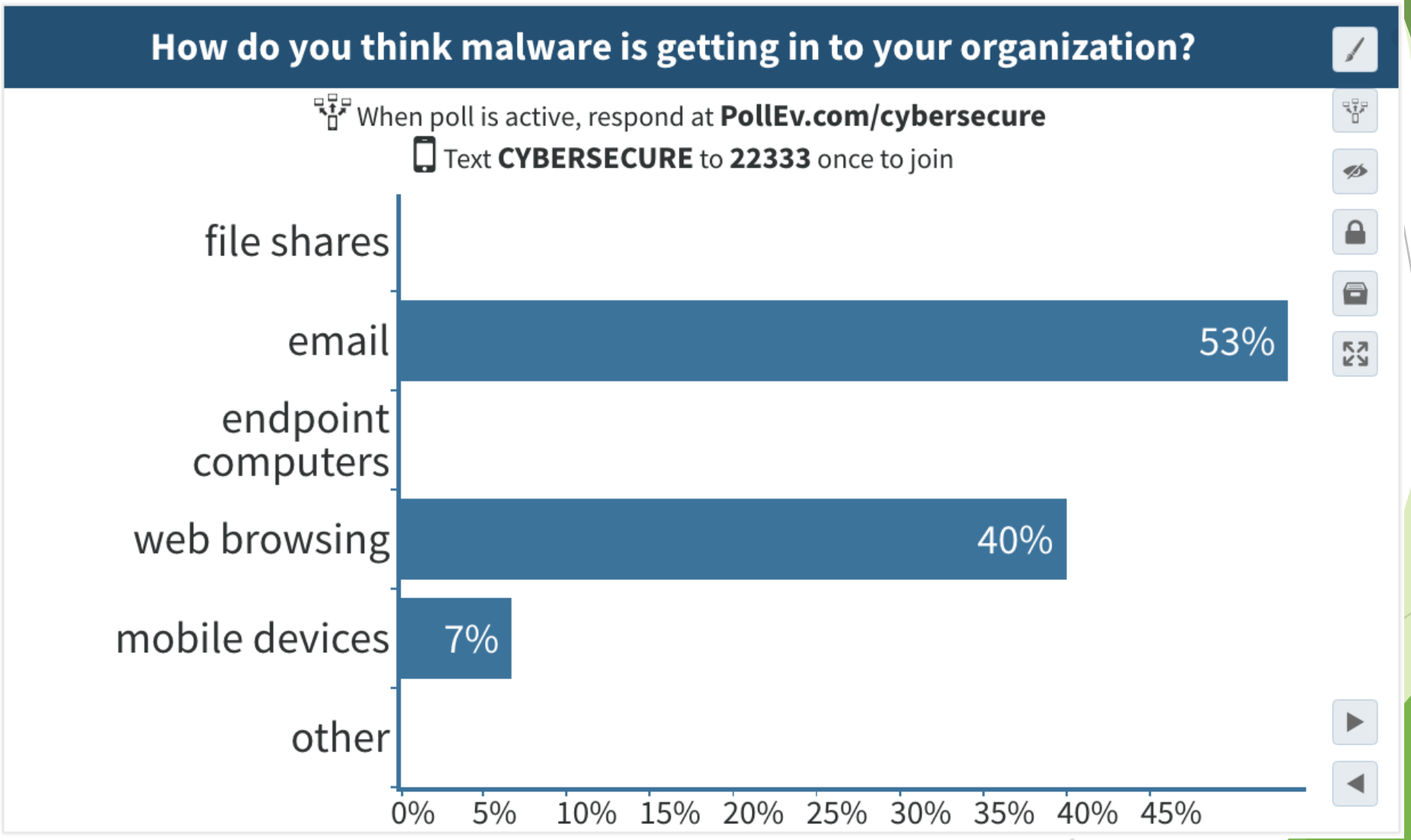
What can we do about all of this? - Hacking

- Protect Assets – firewalls, intrusion prevention, segment networks
- Identify and remediate vulnerabilities –
  - Vulnerability scanning
  - Patch systems and applications





NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

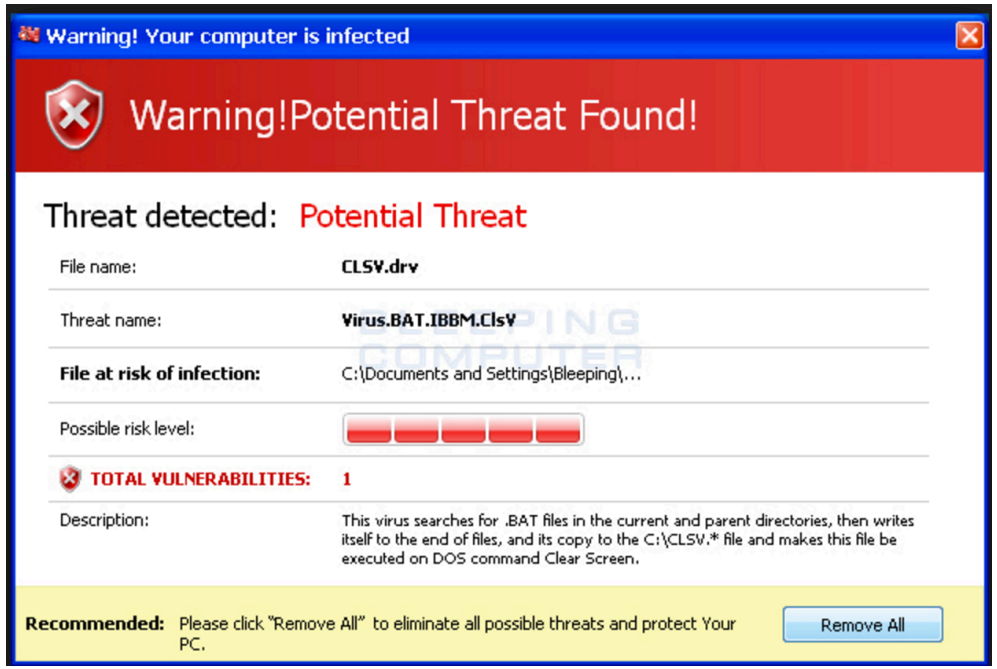


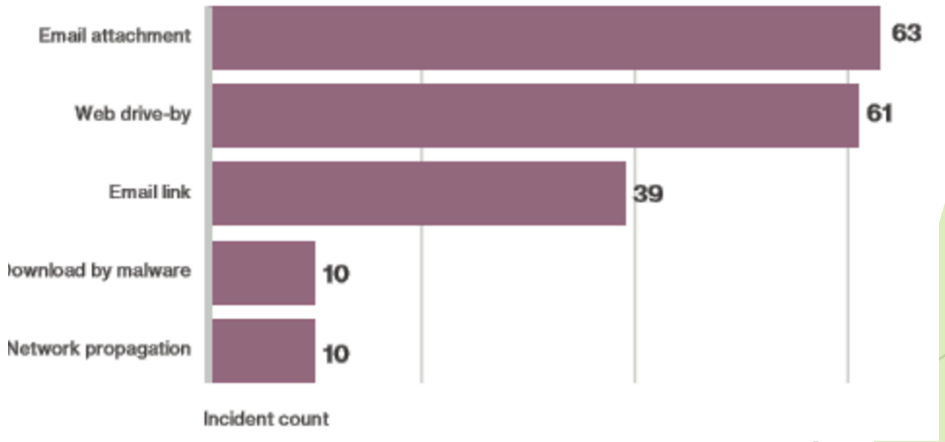
NORTH DAKOTA UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

What can we do about all of this? - Malware

- Patch systems
- Endpoint protection
- Remove/strip executables from email





NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

What can we do about all of this? – Social Attacks- Phishing

- Email/spam filters
- Training/Awareness
- Multifactor Authentication

SANS

Partnership: CIS

NORTH DAKOTA UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Multi-State Information Sharing and Analysis Center (MS-ISAC)

The MS-ISAC is the focal point for cyber threat prevention, protection, response and recovery for the nation's state, local, tribal and territorial (SLTT) governments. The MS-ISAC 24x7 cybersecurity operations center provides real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification, and mitigation and incident response.

Incident Response Services

- No cost
- CERT Incident Response – Computer forensic analysis, malware analysis
- Network and Web Application Vulnerability Analysis
- Cyber Threat Intelligence
- Suspicious email analysis

To take advantage of any of these services, please contact the Security Operations Center (SOC) at soc@cisecurity.org or 1-866-787-4722.

There is **no cost to join the MS-ISAC**, and **membership is open to all SLTT government entities**. The only requirement is the completion of a membership agreement, which outlines member's responsibilities to protect information that is shared.

https://msisac.cisecurity.org/

NORTH DAKOTA
UNIVERSITY SYSTEM
ACCESS. INNOVATION. EXCELLENCE.

Questions?

NORTH DAKOTA
UNIVERSITY SYSTEM

ACCESS. INNOVATION. EXCELLENCE.

What is your favorite ND city?

When poll is active, respond at **PollEv.com/cybersecure** Text **CYBERSECURE** to **22333** once to join

Enable Moderation

↑ Hide poll