BUDGET TRANSFER

Information Systems

DEPARTMENT NAME

JUNE 2018

	Date		Date
Patty Francour	5-9-18	Mark J. Harris	5/10/18
Department Requesting - Signature		Approval - County Executive	
		Approval - Personnel & Finance	6/7/18
Committee of Jurisdiction - Signature			
Committee Vote: Vicky Fitzgerald	5.11.18	Committee Vote: 4-0	
Reviewed by Finance Dept.: N/A		Approved - Information Systems Committee	5-7-18
		Committee Vote: 5-0	
Approved - Facilities & Prop Mgnt Committee			
Committee Vote: N/A		Total amount of budget transfer.....	$45,448

ACCOUNT NUMBER

Org	Object	Project	Phase	Task	Line Description	I=Incr D=Decr	Amount (Whole dollars only)
1039	59999				Undesignated Fund Balance	D	45,448 ~~76,949~~
1022	51100				Regular Pay	I	30,285 ~~52,800~~
1022	51105				FICA	I	2,317 ~~4,001~~
1022	51201				Health Insurance	I	7,057 ~~12,350~~
1022	51206				WI Retirement	I	2,010 ~~3,556~~
1022	51207				Fringe Benefits Other	I	987 ~~1,728~~
1022	51202				Dental Insurance	I	362 ~~634~~
1022	53522				Small Equipment	I	1,100
1022	53008				Telephone	I	475
1022	53006				Computer Software	I	805
					#N/A		
					#N/A		
					#N/A		
					#N/A		
					#N/A		
					#N/A		
					#N/A		

Description (Must be completed - Attach extra pages if needed):

New Position Request - Network Cyber Security Admin - June to December

Revised to cover September through December.

ENTRY NUMBER

Winnebago County

NEW POSITION REQUEST

For 2017 Budget

Department Name: **Information Systems** Org. No.: 22

New Position Title: **Cyber Security Architect**

FT or PT: FT Work Hours per Week: 40 Pay Grade: 27

Brief Description of Duties:

Provides expertise in the planning, implementing, and upgrading of security measures to protect County data and information systems against unauthorized access, modification, or destruction.

Is the new position needed for an existing program? ☐ or a new program? ☐

List Any Position(s) to be Eliminated:

Title	*FTE*

Explain the need for the new program (attach additional pages if needed):

More and more sensitive data is stored on County systems, and hacking/cyber-attacks are increasing exponentially, so departments are relying heavily on IS for security expertise. We do have in-house staff working well outside of their job descriptions in order to attempt to follow best practices for security. It is extremely difficult to carve out time to attend advanced security training with the current workload carried by staff. There are several security-related laws that WC must comply with to avoid monetary penalties or shutdown of certain services.

Identify the consequences if the new position is not approved (attach additional pages if needed):

With the current number of IS employees, and the current workload, we are losing the ability to be proactive. There is not enough time to research and test changes that affect our network which introduces risk. There are plenty of national as well as local examples of security breaches. Just a couple of weeks ago, a Green Bay company's protected personal information was stolen resulting in potential theft of several hundreds of thousands of dollars from employees. In 2016, an Illinois based company was fined $5.55 million for HIPAA violations. Our current security risk assessment shows many shortcomings that need remediation.

Describe the work area, space needs, small equipment needs, computer and software needs, communications equipment needs, and any capital expense associated with the new position (attach additional pages if needed):

The Information Systems department has space to add a person. We would need software licensing for an additional workstation, possibly a new PC, and a phone. We may need cubicle walls, but are willing to utilize some the County may have in-stock.

BUDGET IMPACT

ACCOUNT NAME	ACCOUNT NUMBER	AMOUNT
(1) NEW POSITION LABOR COSTS		
Include all costs for the proposed new postion--do not deduct savings for positions being eliminated.		
Regular Pay	51100	$ 90,855
Overtime	51105	
FICA Medicare	51105	6,950
Health Coverage	51201	21,172
WRS Contributions	51206	6,178
Other Benefits	512xx	2,962
Other (add lines as needed)	51202	1,087
SUBTOTAL		$ 129,204
(2) NON-LABOR COSTS FOR NEW POSITION		
Small Equipment	53522	$ 1,100
Telephone (monthly usage charges)	53008	475
Capital	58xxx	
Computer Software	53006	805
Other (add lines as needed)		
SUBTOTAL		$ 2,380
(3) LABOR COST SAVINGS FROM ELIMINATED POSITION(S)		
Regular Pay	51100	$
Overtime	51105	
FICA Medicare	51105	0
Health Coverage	51201	
WRS Contributions	51206	0
Other Benefits	512xx	0
Other (add lines as needed)		
SUBTOTAL		$ 0
(4) OTHER LABOR COST SAVINGS		
Include items such as reduced OT or hours for other existing employees and temporary help.		
Regular Pay	51100	$
Temporary Help	51101	
Overtime	51105	
Compensatory Time	51108	
Contracted Services		
FICA Medicare	51200	0
WRS Contributions	51206	0
Other (add lines as needed)		
SUBTOTAL		$ 0
(5) REVENUES DUE TO THE NEW POSITION		
Do not include revenue if we would receive it regardless of whether we added new personnel.		
		$
SUBTOTAL		$ 0
NET COST/ (SAVINGS): 1 plus 2 minus 3 minus 4 minus 5		$ **131,584**

memo

Winnebago County Information Systems

To: Mark Harris, Mike Collard, Doug Petraszak

From: Patty Francour

Date: Feb 9, 2018

Re: Request for New Position

Comments: Please find attached the New Position Request Form, a Proposed Job Description, and additional information below.

Most people are very aware of how critical cyber security has become for every industry and every home having Internet access. The IS department works diligently to follow best practices to secure our network to the extent of our abilities while still being prudent with taxpayer money. I would like you to know that we have an extremely talented and dedicated staff; however, there comes a point where retention is a huge deal. I know overtime is a factor in justifying an additional position, but we have a salaried individual putting in many more than 40 hours per week. He also educates and elevates many of the rest of the IS staff with his knowledge and long-time experience here. I would like to alleviate this department's efforts by adding another employee as soon as possible. I would also be happy to discuss in person how valuable a new IS employee is to WC, and what a devastating loss it would be to have anyone go elsewhere. I wish I could put a number on the general increase in complexity of our network from 2001 to today – it is a bit overwhelming how things have changed. This department has had the same number of employees for at least the last 17 years (aside from occasional temp help) while the following changes have occurred:

• 5 servers	255 servers	5000% increase
• 20 switches	156 switches	680% increase
• 687 PCs+laptops+wyse	1193 PCs+laptops+wyse	74% increase
• 0 access points	125 access points	12500% increase
• 0 tokens	200 tokens	20000% increase

- Number of applications, licensing requirements, compliance!

In the IS department, it takes a lot of time, effort, and money to groom an employee before the County reaps a return on its investment. Managing, grooming, and retaining "talent" is a big challenge, and it costs dearly if valuable employees decide to go elsewhere. I feel the County overall would benefit if IS could add a staff member focused primarily on security. We've learned some unsettling things from a current, local security incident. The disabled institution had difficulty even finding *vendors* in the region that were capable of providing help. Also, a federal security assistance organization is currently backlogged 4-6 weeks. Below are a few examples showing the frequency and difficulty in resolving recent attacks. Please note all of the headlines included are from 2018.

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

By Kimberly Hutcherson, CNN
Updated 3:00 PM ET, Wed March 28, 2018

Story highlights

City employees were told to turn their computers on Tuesday for the first time since the cyberattack

Public safety services and airport functions remain unaffected, city officials say

Atlanta (CNN) — Residents can't pay their water bill or their parking tickets. Police and other employees are having to write out their reports by hand. And court proceedings for people who are not in police custody are canceled until computer systems are functioning properly again.

More than six days after a ransomware attack shut down the city of Atlanta's online systems, officials here are still struggling to keep the government running without many of their digital processes and services.

The city said on Twitter that all court dates set for Wednesday will be rescheduled and all applications for jobs with the city are suspended until further notice.

On Tuesday officials told city employees to turn their computers and printers back on for the first time, part of an ongoing assessment of the impacts of the cyber breach, which took place on March 22.

LILY HAY NEWMAN SECURITY 04.23.18 08:55 PM

ATLANTA SPENT $2.6M TO RECOVER FROM A $52,000 RANSOMWARE SCARE

UW experts reflect on Atlanta ransomware attack, what it could mean for Madison

In light of destructive Atlanta cyber attack, UW experts call for change in local municipalities', UW security

Ransomware is a newer type of cyber attack, which disables systems until a ransom is paid to get it back, said Dave Schroeder, technology and cybersecurity strategist for the University of Wisconsin Division of Information Technology.

"There is generally no way to recover data from this kind of attack without knowing the decryption key, which the attackers will only provide if the ransom is paid, or by recovering systems from backups," Schroeder said. "Even with good backups, this can be a painstaking and time-consuming process. Often the ransom amounts may not seem large by US standards, but could represent a windfall for attackers operating in other parts of the world. The attackers usually demand the ransom be paid using cryptocurrencies like Bitcoin."

"This kind of attack could happen anywhere," Schroeder said. "Any city service that depends on computers could be impacted, from the water utility to police and fire service to the Madison schools. These kinds of attacks can impact an entire city's population, with days to weeks to fully recover. This is why it is really incumbent on any organization to recognize that while good cybersecurity policies and practices cost money to implement, they can save even more money in the long run."

The New York Times

By Nicole Perlroth

March 28, 2018

Boeing said on Wednesday that it was hit by a cyberattack that some Boeing executives identified as the same WannaCry computer virus that struck thousands of computer systems in more than 70 countries around the world last year.

In an internal memo, Mike VanderWel, chief engineer of Boeing Commercial Airplane production engineering, said the attack was "metastasizing" and he worried it could spread to Boeing's production systems and airline software.

"We are on a call with just about every VP in Boeing," Mr. VanderWel wrote. The memo called for "All hands on deck."

WannaCry is a particularly vicious form of what is known as ransomware — malware that locks up victims' computers and data with encryption, until attackers' extortion demands are met, often in the form of the virtual currency Bitcoin. Even for victims who agree to pay, decryption is not always guaranteed. The City of Atlanta was hit with a different form of ransomware last week and was still reeling from the fallout on Wednesday.

Feb 25 2018

UK: Hackers break into schools' CCTV system and stream footage of pupils live on the internet

Posted by Dissent at 11:41 pm Education Sector, Non-U.S.

James Tozer reports:

> Happily chatting and walking between lessons, these children are being watched by school spy cameras designed for their protection.
>
> Now it has emerged that the images can be viewed by anyone after the CCTV systems were hacked and put online.
>
> A disturbing website, which boasts 'Watch live surveillance cameras in the UK', allows people anywhere in the world to spy on children, teachers and parents in real time.

Connecticut agencies hit with WannaCry

By Matt Leonard Feb 26, 2018

Connecticut is not alone in its fight against cyberattacks. The Colorado Department of Transportation and the city of Allentown, Pa. experienced large breaches earlier this month, according to SC Media.

CDOT was able to restore its system from backups. But the malware attack in Allentown could cost the town $1 million, according to the Allentown Morning Call.

By **Daniel Patrick Sheehan, Emily Opilo and Daryl Nerl · Contact Reporters**
Of The Morning Call

FEBRUARY 20, 2018, 7:10 PM

A serious computer virus that has struck the city of Allentown's most critical systems is expected to cost nearly $1 million to remove and has forced the city to shut down some financial and public safety operations, Mayor Ed Pawlowski announced Tuesday.

The malware virus, known as Emotet, first attacked the city a week ago and has been self-replicating, stealing credentials such as passwords for city employees, Pawlowski said during an unannounced update to Allentown City Council delivered during an unrelated confirmation hearing.

Representatives from Microsoft have been hired by the city for an initial $185,000 emergency response fee, and the virus has been contained, Pawlowski said. However, it will cost an additional $800,000 to $900,000 for a recovery phase that will repair the damage that the virus has done, he said.

INDUSTRY NEWS

SamSam ransomware infects Colorado Department of Transportation

3 months ago 2 Min Read

SamSam ransomware is back and the Colorado Department of Transportation is its most recent victim. More than 2,000 agency computers had to be shut down on Feb 21 to prevent the ransomware from spreading across the entire infrastructure.

Colorado Department of Transportation is one of the many organizations that fell victim to SamSam ransomware that in January infected vulnerable networks in hospitals, city councils, educational facilities and transportation systems.

Following its infection with SamSam and the encryption of over 1,400 files, a hospital in Indiana paid $55,000 to restore its systems. In that case, although they had data backups, they chose to pay the ransom. SamSam doesn't spread via phishing campaigns but takes advantage of unsecured devices directly connected to the internet and uses them to spread laterally across the network.

By Ben Coley / The Dispatch
Posted Feb 16, 2018 at 10:12 AM
Updated Feb 19, 2018 at 9:34 AM

The Davidson County government's ability to conduct business on computers has been stopped by a virus known as ransomware, an issue that could take weeks or months to fully resolve, according to County Manager Zeb Hanner.

The Davidson County Board of Commissioners held an emergency meeting at 2 p.m. Friday to discuss the cyber attack.

Joel Hartley, Davidson County's chief information officer, said that at 2:30 a.m. Friday, he was notified by the 911 director that the department had suspicious activity within its system. Officials soon discovered that the county had been compromised by ransomware called Samas.

Hartley said the virus has impacted more than 70 servers and an unknown number of desktops and laptops. None of the phone systems for county offices are working, either. He added that staff is currently searching for the source of the virus to isolate it and start recovery efforts.

Sensitive info may be compromised after City of Houston employee's laptop stolen

City officials say the laptop was stolen from the employee's car on Feb. 2. They say the password-protected computer may have contained records, including names, addresses, dates of birth, Social Security numbers and other medical information.

Author: KHOU.com Staff
Published: 5:47 PM CST February 23, 2018
Updated: 5:47 PM CST February 23, 2018

City officials say human resource professionals are trained not to remove laptops from City offices unless sensitive data is encrypted. They say one employee "failed to follow his training."

"Because one employee failed to follow his training, all employees authorized to work with group health plan data are being retrained to reinforce the prohibition against removing unencrypted data from the protections of City facilities," City officials said in a statement. "Potentially affected employees, retirees, and their dependents will receive a letter notifying them of the potential breach. Because Social Security numbers were involved, it is recommended that those who receive a notice place a fraud alert on their credit files."

The City is providing free credit monitoring and identity restoration services for one year to help protect personal information. Those with questions on this case may contact the City at 1-855-288-3409.

19.5M California Voter Records Breached After Ransomware Infection

February 9, 2018 Kayla Elliott 2 Comments

Baltimore's 911 Systems Down After Ransomware Infected Systems

March 30, 2018 Kayla Elliott 1 Comment

Social Security numbers from thousands of California state workers exposed in data breach

BY ADAM ASHTON
aashton@sacbee.com

February 16, 2018 03:40 PM
Updated February 20, 2018 09:36 AM

Social Security numbers for thousands of state employees and contractors were exposed in a recent data breach at the Department of Fish and Wildlife, according to a memo that the department sent to its workers this week.

The department discovered the data breach on Dec. 22, but did not disclose the breach to employees until this week. The California Highway Patrol has been investigating the incident for the past two months.

According to the memo, a former state employee downloaded the data to a personal device and took the records outside of the state's network. The memo does not say when or why the former employee downloaded the information to an unsecured network.

Russian computer hackers in Colorado sold stolen credit card numbers for $3.6 million

Feds file forfeiture claims against two Colorado bank accounts implicated in the investigation

By KIRK MITCHELL | kmitchell@denverpost.com | The Denver Post
PUBLISHED: February 26, 2018 at 11:00 am | UPDATED: February 26, 2018 at 6:00 pm

Russian computer hackers operating in Colorado and 15 other states used data-mining viruses to steal thousands of credit card numbers from U.S. residents in 20 states and sold them on the darknet for more than $3.6 million, according to federal court documents.

Ransomware Takes Down Oregon Public School

May 9, 2018 Kayla Elliott Leave a comment

California Medical Facility Notifies Patients of Breach, Post-Ransomware Infection

April 27, 2018 Kayla Elliott 1 Comment

Massachusetts School Pays Hackers – Still Waiting for Data

April 27, 2018 Kayla Elliott 1 Comment

Georgia Faces Yet another Ransomware Attack

April 25, 2018 Kayla Elliott Leave a comment

Ransomware Riddles Massachusetts Town Office

April 23, 2018 Kayla Elliott Leave a comment