Legislative Fiscal Bureau
One East Main, Suite 301 • Madison, WI 53703 • (608) 266-3847 • Fax: (608) 267-6873
Email: fiscal.bureau@legis.wisconsin.gov • Website: http://legis.wisconsin.gov/lfb

June, 2023 | Joint Committee on Finance | Paper #282

Cybersecurity
(Children and Families -- Child Support and Departmentwide)

[LFB 2023-25 Budget Summary: Page 124, #7]

CURRENT LAW

The state's largest information technology (IT) systems store a vast amount of sensitive data, including personally identifying information and financial records. The Department of Children and Families (DCF) is responsible for managing several major IT systems, including: (a) the Child Care Statewide Administration on the Web (CSAW), used for the Wisconsin Shares; (b) the Kids Information Data System (KIDS), used for child support enforcement; (c) the Benefit Recovery Information Tracking System (BRITS), used for investigating and recovering improper benefits payments; (d) the Client Assistance for Reemployment and Economic Support (CARES) system, used for public assistance eligibility determinations and case management functions; (e) eWiSACWIS, used for child welfare and youth justice services; and (f) virtual desktops used by DCF staff. (A virtual desktop is a pre-configured image of an operating system or application in which the desktop environment is separated from the physical device used to access it, enabling users to access their desktop environments remotely over a network.) Each system stores personally identifiable information and interfaces with both internal and external systems and users.

For example, DCF manages the centralized receipt and disbursement function statewide for child support payments. A vendor receives all child support payments from employers and individuals and then passes a file to the state. The state interfaces the information into KIDS, which determines monthly child support payment amounts. Child support payments are then distributed to the appropriate payees (usually an electronic form of payment). A data breach of state systems could potentially disrupt child support payment activities or personal information across the state.

DCF indicates that it is currently in compliance with Wisconsin's basic information

technology security policies and standards. DCF provides annual training to encourage employees to recognize, avoid, and report cybersecurity incidents, and automatically backs up critical systems on a regular schedule. DCF reports that it has prevented individual cyberattacks with current funding in the program divisions information technology budgets.

DISCUSSION POINTS

1. State and local agencies must prepare for several kinds of potential cybersecurity threats. Malware (such as viruses, Trojan horses, and worms) is software designed to harm computer systems by destroying or altering data, or collecting user activity data without the users' knowledge. Phishing attacks can trick users into revealing confidential information (such as passwords or financial information). Denial-of-service attacks can overwhelm a network with a large number of requests or data, rendering the computer system unavailable to users. Ransomware can encrypt a computer system's files, holding critical information hostage for payment. Because of the nature of cybersecurity threats, a vulnerability in a small system can compromise more critical areas of a network.

2. A data breach can have a severe impact on users and an agency's reputation. Hackers can use stolen data to steal a user's identity to apply for credit cards and loans in the victim's name. A data breach can disrupt government services by bringing down the network. For example, the Legislative Reference Bureau (LRB) report entitled, Ransomware Attacks: Lessons for Wisconsin State and Local Government, noted that in 2019, ransomware attacks inflicted costs of more than $7.5 billion nationwide on government-related entities, affecting at least 113 state and municipal government and agencies, 764 health care providers, and 89 universities, colleges, and school districts. In 2020, the computer systems of cities of Racine and Oshkosh were compromised within days of each other, preventing the cities from accepting electronic utility payments, which required residents to remit utility bill payments through mail or in person.

3. According to the LRB report Data Breaches: Risk, Recovery, and Regulation, most data breaches are motivated by profit via direct theft of financial data or by stealing other data that can be used for identity theft or sold to others looking to profit from it.

4. Cybersecurity threats and attacks have been on the rise nationally. A 2018 IBM/Ponenmon Institute study predicted that the average probability of a significant breach at any given organization would be nearly 28% over the next two years. In 2021, a security report by CrowdStrike found that cybersecurity threats, including hacking efforts, grew by 400% in 2019 and 2020 combined. These incidents are anticipated to continue to grow as advances in, and reliance on, technology increase. In particular, cybersecurity threats may become more prominent as DCF upgrades its systems to transition away from mainframe systems to toward modern information technology systems utilizing expanded communication abilities.

5. Having a cybersecurity plan in place to identify and mitigate potential risks can help protect sensitive data, avoid disruption of essential services, minimize the impact of data breaches, and maintain user trust in the security of their information. For instance, investing in training for staff can help to prevent human error, which causes a significant portion of data breaches. In the long run,

a cybersecurity plan can reduce costs by preventing cyberattacks from inflicting damage in the first place.

6. DCF indicates that, to date, it has prevented cyberattacks with base funding budgeted for information technology services. However, there is not enough base funding to strengthen an agency-wide response or explore newer technologies. DCF indicates that it expects cyberattacks to become more frequent and more sophisticated with hackers exploiting micro-level vulnerabilities to access the larger system behind applications. Because any breach could potentially leave all programs vulnerable, DCF recommends a comprehensive agency-wide response.

7. AB 43/SB 70 would increase funding for the agency's general administration appropriation by $1,185,800 GPR annually to develop and implement a comprehensive cybersecurity plan for infrastructure, data, systems, and user accounts. The plan would include the following elements: (a) proactively managing, monitoring and tracking IT systems; (b) backup and recovery of critical systems and data; (c) strengthening digital data integrity and interoperability; (d) support for a contracted privacy officer to review data confidentiality; (e) cybersecurity supervision and coordination; and (e) implementation of a single "MyWisconsin" ID and authentication across state IT system.

8. Table 1 summarizes the component parts of the Administration's plan, including DCF's estimates of the annual cost of each component. Under the plan, staffing for implementation of the plan would entail six contract positions and one consultant. No additional state positions would be authorized. Cybersecurity would be analyzed, reviewed, and provided on a centrally for all DCF systems from the Division of Management Services.

TABLE 1

DCF Cybersecurity Plan Budget
AB 43/SB 70

	Annual Funding
Security and architecture team to proactively manage, monitor, and track IT systems	$352,800
Staffing to explore technologies for backup and recovery of critical systems and data; manage incident response	117,600
Staffing to strengthen digital data integrity and interoperability; Digital data exchange – security/standards	264,600
Dedicated DCF privacy officer to review data confidentiality	175,000
Cybersecurity supervision/coordination	75,800
Staffing to implement a single MyWisconsin ID and authentication across all state information systems.	200,000
Total	$1,185,800

9. If the Committee wished DCF to implement the cybersecurity plan, it could choose to fund it by drawing funding from several funding sources and programs that use DCF's IT systems. Under this option, budget authority would be increased in several different GPR, FED, and PR appropriations and then transferred for centralized services. DCF has identified the following sources that could be used to support the plan, as shown in Table 2.

TABLE 2

Allocation of Cybersecurity Plan Funding Among Divisions and Programs

		Source	Amount
	Children and Family Services		
(1)(aw)	General Program Operations	GPR	$124,500
(1)(cw)	Milwaukee Child Welfare Services	GPR	313,100
(1)(mw)	Milwaukee Child Welfare Services	FED	29,500
(1)(n)	State Foster Care and Adoption Services	FED	76,300
	Economic Support		
(2)(a)	General Program Operations	GPR	26,200
(2)(jn)	Child Care Licensing and Certification Activities	PR	24,500
(2)(mc)	Federal Block Grant Operations	FED	376,900
(2)(n)	Child Support State Operations	FED	52,700
(2)(om)	Refugee Assistance	FED	14,400
(2)(mc)	Federal Block Grant -- State Operations (TANF)	FED	127,400
	General Administration		
(3)(a)	General Program Operations	GPR	20,300
	Subtotal		$1,185,800
(3)(k)	**Administrative and Support Services**	PR	$1,185,800

10. Under this alternative, the cybersecurity plan would be support with $484,100 GPR, $677,200 FED, and $24,500 PR annually. These costs would be "double counted" in the DCF budget, as funding would be transferred to a program revenue-service appropriation that funds centralized administrative and support services

11. Providing GPR funding to support a comprehensive cybersecurity plan is appropriate because GPR can be used to support any or all its programs at any given time, unlike single program fund sources. DCF seeks flexible funding for cybersecurity that is able to pivot and work on any number of efforts during a fiscal year, ranging from proactive implementation to data breach response. GPR can cover all of DCF's programs and be applied to security threats in any of its computer systems. According to DCF, federal cost allocation agreements are more limited with the use of PR funding.

ALTERNATIVES

1. Provide $1,185,800 GPR annually for DCF to develop and implement a comprehensive cybersecurity plan for critical infrastructure, data, systems, and user accounts across all of its information technology systems.

ALT 1	Change to Base
GPR	$2,371,600

2. Provide $1,185,800 ($484,100 GPR, $677,200 FED, and $24,500 PR) annually for DCF to develop and implement a comprehensive cybersecurity plan for critical infrastructure, data, systems, and user accounts across all of its information technology systems. Allocate funding for the program as shown in Table 2.

ALT 2	Change to Base
GPR	$968,200
FED	1,354,400
PR	2,420,600
Total	$2,371,600

3. Take no action.

Prepared by: John D. Gentry