디지털 위험이 곧 비즈니스 위험

기관의 임무에 영향을 미치는 IT 현대화의 동향

연방 기관(민간 기관 또는 국방 기관 및 정보 기관 등)에서 정부 및 지자체에 이르기까지 공공 부문의 조직은 더 나은 주민 서비스를 제공하고, 국토를 보호하고, 시민과 데이터를 연동하고, 기관의 효율성을 높이기 위해 디지털 혁신을 추진하고 있습니다.

이러한 디지털 혁신은 하룻밤 사이에 이루어지지 않습니다. 디지털 혁신은 기관 차원의 CIO를 설립해 IT 현대화를 감독하고 실현하는 1990년대 입법(1996년 클린저-코헨 법)[1]으로 시작되어 인터넷 사용을 촉진해 시민의 정부 참여를 높이는 2002년[2] 전자정부법을 통해 지속되었으며, 정부의 혁신에 따라 적절한 보안 조치를 이행하는 2002년 FISMA(Federal Information Security Modernization Act) 입법으로 이어졌습니다. 최근 클라우드 우선[3] 및 클라우드 스마트[4]와 같은 정책 및 표준에 힘입어 정부 조직이 빠르게 디지털 혁신을 추진하고 있습니다. 또한 행정 명령은 행정부의 사이버 관련 의제를 설명해 왔습니다. 이러한 모든 변화 속에서 정부의 IT 및 보안 전문가는 시스템 및 데이터를 안전하게 유지하고 중요한 정부 및 시민 데이터를 보호하는 동시에, 이해 관계자에게 개방적이고 투명한 상태를 유지해야 하는 과제를 담당합니다.

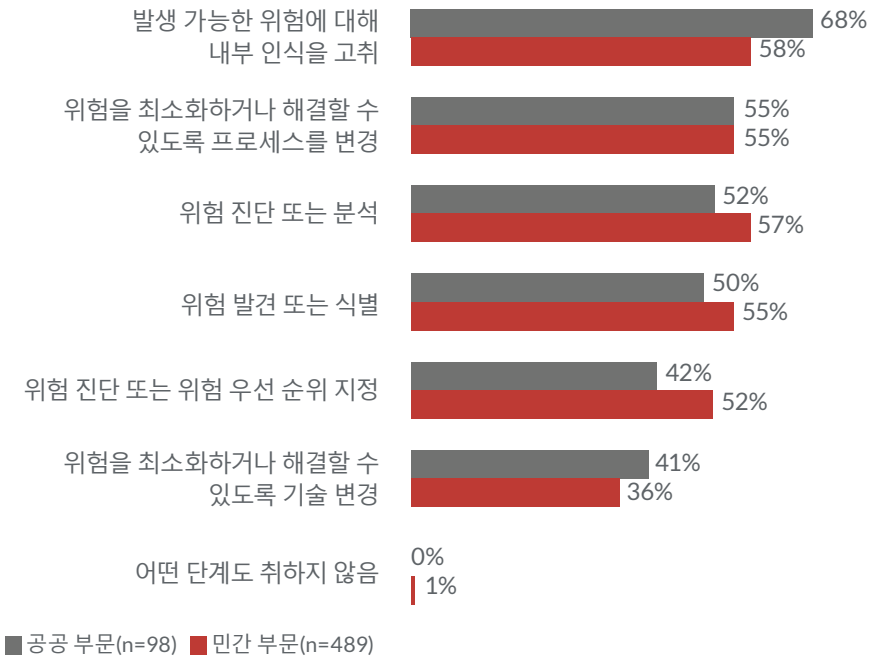
기관과 그 파트너가 온라인 및 모바일 환경을 통해 정부가 시민에게 더 쉽게 접근할 수 있도록 노력하는 과정에서, 이러한 활동으로 인해 운영 및 데이터가 사이버 공격에 취약해질 위험도 있습니다.

독립적으로 그리고 다른 조직(공공 및 민간)과 협력하여, 주민에게 맡은 임무의 성과를 제공하고자 디지털 혁신을 추구하는 정부 조직은 임무에 영향을 미칠 수 있는 위험이 잠재적으로 증가할 수 있는 상황에 직면하고 있습니다. 기관과 파트너가 온라인 및 모바일 환경을 통해 정부가 시민에게 더 쉽게 접근하도록 노력함에 따라, 이러한 작업으로 인해 국가, 활동가, 불만 있는 시민 등 혼란을 초래하려 하는 외부의 위협 요소나 내부자의 위협을 통한 사이버 공격으로 인해 운영 및 데이터가 취약해질 위험 또한 존재합니다. 이는 잠재적으로 다음과 같은 중대한 영향을 미칠 수 있습니다.

- 국가 안보에 대한 위협
- 공공 서비스, 공익 사업 및 의료 서비스 중단
- 개인정보 침해, 보안 침해 및 다크 웹 범죄자에게 수백만 시민의 개인 및 금융 데이터 유출
- 기밀 정보의 유출로 인해 국제적 또는 국내적 혼란, 경제 무역 영향, 그리고 군을 위험에 빠뜨릴 수 있는 가능성 초래
- 합법적인 선거에서 유권자의 신뢰를 무너뜨리는 선거 조작

공공 부문의 조직은 디지털 위험의 심각성을 통감하고 이를 최소화하기 위한 조치를 취하고 있습니다. 2019년 RSA 디지털 위험 보고서에 포함된 RSA 디지털 위험 연구 결과에 따르면, 공공 부문에 종사하는 68%의 응답자가 내부적으로 디지털 혁신 시 발생할 수 있는 위험에 대한 인식을 제고하기 위해 조치를 취했다고 응답한 반면, 민간 부문 조직 응답자의 경우 58%에 불과했습니다. 이러한 사실은 위협 요소로부터 자신, 정부 데이터 및 시스템을 보호하는 방법과 위험에 대한 인력 교육 측면에서 공공 부문 조직이 민간 부문 조직보다 더 높은 성과를 거두고 있다는 것을 의미합니다.

디지털 위험 관리를 위한 단계



2019년 RSA 디지털 위험 보고서에 포함된 RSA 디지털 위험 연구 결과에 따르면, 공공 부문에 종사하는 68%의 응답자가 내부적으로 디지털 혁신 시 발생할 수 있는 위험에 대한 인식을 제고하기 위해 조치를 취했다고 응답한 반면, 민간 부문 조직 응답자의 경우 58%에 불과했습니다.

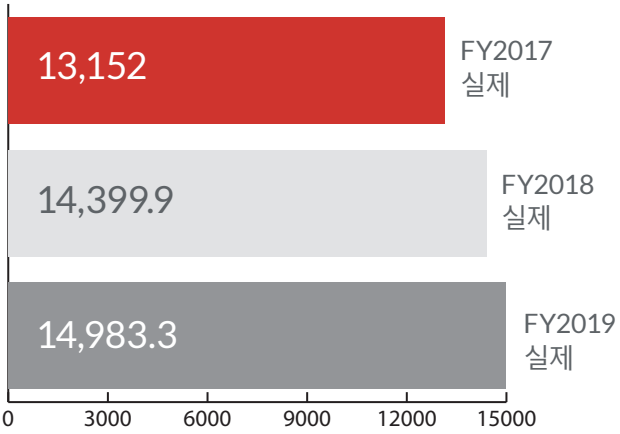
또한 공공 부문 응답자는 향후 2년 동안 가장 관심을 기울여야 할 디지털 위험의 상위 세 가지 영역, 즉 사이버 공격의 위험, 데이터 프라이버시 위험 및 역동적인 업무 환경의 위험에 대해 인지하고 있었습니다.

사이버 공격 위험

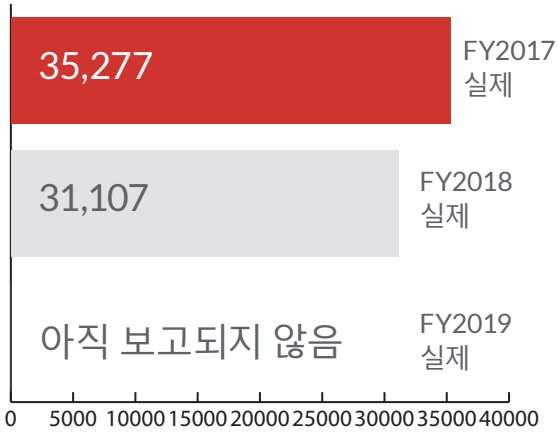
RSA 디지털 위험 연구에 따르면 지난 2년간 공공 부문에서 가장 중요한 위험 관리 목표는 사이버 공격의 최소화였습니다. 이 위험 관리의 중요성은 미국 GAO(Government Accounting Office)의 FISMA 회계연도 2018 미 의회 제출 연례 보고서에 잘 나타나 있습니다. 이 보고서에 따르면 사이버 보안 인시던트가 이전 회계연도(2017 회계연도에 35,277건 발생)보다 12% 감소하는 등 사이버 공격 위험 관리에 상당한 진전을 보이고 있습니다. 그러나 또한 이 보고서는 2018 회계연도에 여전히 31,107건이 넘는 사이버 보안 인시던트가 있었다는 사실을 강조합니다.[5] 이러한 사실은 연방 기관이 정보와 시스템을 위협 요소로부터 보호하는 데 큰 어려움에 직면하고 있다는 것을 보여주며, 사이버 보안 문제는 연방 정부에 "고

기관의 사이버 보안 투자금 총액

(단위: 백만 달러)



FISMA에 보고된 사이버 인시던트 수



출처: https://www.whitehouse.gov/wp-content/uploads/2017/11/FY2017FISMAReportCongress.pdf

위험 문제"가 되고 있습니다.[6] 보다 최근에 발표된 GAO 보고서에서는 "국가의 사이버 보안 강화"를 행정부와 의회에서 경각심을 갖고 특별히 중점을 두는 9개의 고위험 영역 중 하나로 꼽았습니다.[7]

현재 사이버 보안 문제를 겪고 있는 공공 부문이 연방 기관만은 아닙니다. 올해 초, 텍사스에 이어 22개 자치단체에 랜섬웨어 공격이 발생했으며, 이와 비슷한 시기에 볼티모어, 조지아주 법원 시스템, 유타주 내 한 지방의 데이터 네트워크도 공격받았습니다.[8] 공격자는 지방 정부가 사이버 보안에 투자할 리소스를 더 적게 보유하고 있다고 간주하므로 지방 정부가 연방 기관보다 이러한 유형의 공격에 더 취약하다는 합리적인 추측이 가능합니다. 이러한 공격 유형 중 많은 수가 증가하고 있으나[9], 정부 및 지자체는 이에 따른 조치를 취하고 있습니다. 예를 들어 텍사스 주의 경우 민간 공급업체와 협력하여 다른 툴 및 지원과 함께 사이버 보안 서비스 및 MSS(Managed Security Service)를 제공함으로써 지방 정부와 공공 기관이 보안 툴, 모니터링 및 탐지 기능을 비용 효율적으로 사용할 수 있도록 지원하고 있습니다.[10] 또한 정부 및 지자체는 교육의 질을 높여 사이버 보안에 대한 인식을 제고할 수 있는 모범 사례를 통해 인력을 교육하고 있습니다. 사용자에게 피싱 이메일과 이를 인지하고 이에 대응하는 방법을 알려주는 등의 간단한 교육으로도 잠재적인 위협을 인지하고 유사한 피싱 기반 공격을 방지하는 방법을 제공할 수 있습니다.

공공 부문 조직은 예산 및 리소스 제약으로 인한 어려움을 극복하면서 전반적인 사이버 보안 태세를 지속적으로 개선하고 있습니다. 정부 기관은 사이버 공격에 대한 식별, 탐지, 보호, 대응 및 복구를 수행할 수 있는 기술, 인력 및 프로세스에 중점을 두는 NIST(National Institute of Standards and Technology)의 CSF(Cyber Security Framework) 등 사이버 보안을 위한 공통 프레임워크를 도입하고 있습니다. 조직은 가장 중요한 위협의 우선 순위를 지정할 수 있도록 자동화 및 지능형 공격 탐지 기능을 구현하는 위험 기반 접근 방식을 취하고 있습니다. 또한 정부의 보안 책임자는 정부 정보에 사용자 본인만 액세스할 수 있도록 다단계 인증, ID 거버넌스 및 수명주기 관리와 같은 기본적인 보안 보호 기능을 지속적으로 구현 및 개선하고 있습니다.

정부의 보안 책임자는 정부 정보에 사용자 본인만 액세스할 수 있도록 다단계 인증, ID 거버넌스 및 수명주기 관리와 같은 기본적인 보안 보호 기능을 지속적으로 구현 및 개선하고 있습니다.

역동적인 업무 환경의 위험

오늘날의 공공 서비스 업무 환경은 극적으로 변화하고 있습니다. 더 많은 밀레니엄 세대가 공공 서비스에 종사함에 따라 정부 공무원의 인구통계학적 변화가 일어나고 있을 뿐 아니라, 신뢰를 바탕으로 한 많은 수의 계약업체들이 지속적으로 임무를 지원하고 있습니다. 민간 부문과 마찬가지로, 공공 부문 조직에서도 더 많은 디지털 기술을 도입하여 직원이 보다 생산적이고 효과적으로 임무를 달성할 수 있도록 지원하고 있습니다. 그러나 이로 인해 정부 보안 및 위험 관리 책임자는 시민 및 정부 데이터 보호에 필요한 보안 명령과 리소스 제어에 따라 다양한 업무 환경 내 디바이스, 플랫폼 및 클라우드에 있는 정보의 개방적 흐름과 유동적 흐름을 밸런싱해야 하는 당면 과제를 안게 됩니다.

공공 부문 생태계 전반에서 액세스 및 ID 보증을 실현하기 위해 기관에 추가적인 요구사항을 두는 규제 명령, 기관 및 행정부 차원의 명령으로 인해 이러한 당면 과제는 더 복잡해지고 있습니다. 균형 관리를 위한 정책도 변화하고 있습니다. 정부는 수년 동안 내부자 위협 프로그램을 시행해 왔으나, 내부자 위협의 개념이 변하고 있습니다. 모바일 디바이스와 클라우드에 점점 더 많은 정부 데이터가 저장됨에 따라, 악의는 없더라도 부주의한 실수 등으로 인해 직원이나 계약업체가 취약점을 노출시킬 수 있습니다. 정부에서 지급한 노트북을 버스에 두고 내리기, PIV 카드를 원래 위치에 두지 않기, 정부에서 지급한 디바이스에서 개인 디바이스 또는 다른 작업 디바이스로 데이터를 전송하여 작업을 완료하기 등과 같은 행위는 모두 단순한 실수에 불과하더라도 데이터의 손실을 야기할 수 있는 실질적인 위험 요소에 해당합니다. 공공 부문 조직은 교육과 인식 제고를 통해 이 문제를 해결하고자 많은 노력을 기울이고 있습니다. 앞서 언급한 바와 같이 RSA 디지털 위험 보고서의 분석 결과 중 하나는 이러한 디지털 위험에 대한 인력의 인식 제고 측면에서 공공 부문 조직이 민간 부문보다 더 나은 성과를 거두고 있다는 점입니다. 모든 공무원과 계약업체가 정부 데이터 및 리소스 보안에 대한 책임 의식을 갖추도록 하려면 지속적인 경계와 교육이 중요합니다.

정부 조직은 액세스 제어 방식을 개선하여 누가 데이터에 액세스할 수 있는지, 데이터를 이용해 어떤 작업을 하는지에 대한 가시성을 제공함으로써 데이터 프라이버시 위험을 해결하기 위해 지속적으로 노력할 뿐만 아니라 인력 및 시민의 개인정보 보호를 위해 데이터 관리 정책을 발전시키고 있습니다.

마지막으로, 기관의 보안 책임자가 업무 환경의 생산성을 높이기 위해 배포하는 툴도 진화하는 중입니다. 보안 책임자는 기존의 액세스 제어 방식(CAC/PIV)을 보완하고, 최신 인증 방식을 사용해 액세스를 간소화하는 다단계 인증, 모바일 푸시, 생체 인식 등의 다른 제어 방식을 도입하고자 합니다. 이는 직원이 수행해야 하는 액세스 권한 프로세스를 간소화하면서도 각 시스템에 대해 액세스 제어를 보장합니다. 백엔드에서 위험 기반 분석을 활용하면 직원 사용자를 번거롭게 하지 않는 새로운 방식으로 부적절한 액세스를 모니터링하고 탐지할 수 있습니다.

데이터 프라이버시 위험

데이터 프라이버시는 모두의 관심사입니다. 상업 부문에서 발생하는 보안 침해가 사회적인 문제로 헤드라인을 장식하고 있지만, 공공 부문 조직도 예외는 아닙니다. 2019 Verizon Data Breach Investigations Report에서는 데이터 침해의 16%가 공공 부문에서 발생했다고 밝히고 있으며, 이는 의료 부문에서의 비율과 거의 동일합니다.[11] National Law Review에서는 특히 수백만 개의 신원 조사 기록 및 인력 기록 파일이 유

출된 2019년 OPM(Office of Personnel Management) 보안 침해 사건 이후, 공공 부문의 데이터 프라이버시 위험에 대해 보다 앞으로 보다 중요하게 취급해야 할 위험이라 설명하고 있습니다.[12]

OPM 보안 침해 사건의 규모는 정부 시스템에 있는 개인 데이터가 얼마나 위험에 처해 있는지 실감하게 만듭니다. 정부 시스템에는 연방 정부의 종사자 또는 수백만 명의 지원자들의 데이터 외에도 수백만 명분의 데이터가 저장되어 있습니다. 정부 조직의 임무는 시민에게 봉사하는 것입니다. 따라서 정부는 시민의 신뢰에 대한 보답의 일환으로 시민의 데이터를 안전하게 보호하고 의도된 목적으로만 사용해야 합니다. 이는 임무의 성공에 있어 매우 중요합니다.

바람직한 소식은 정부 조직이 액세스 제어 방식을 개선하여 누가 데이터에 액세스할 수 있는지, 데이터를 이용해 어떤 작업을 하는지에 대한 가시성을 제공함으로써 데이터 프라이버시 위험을 해결하기 위해 지속적으로 노력할 뿐만 아니라 인력 및 시민의 개인정보 보호를 위해 데이터 관리 정책을 발전시키고 있다는 점입니다. 예를 들어, 국세청은 납세자 인증을 위해 주민 등록 번호 사용을 최소화하는 프로그램을 도입했습니다.[13] 그리고 NIST에서는 기존 NIST CSF와 마찬가지로 공공 기관은 물론 민간 비즈니스에도 적합한 모델이 될 수 있는 데이터 프라이버시용 프레임워크를 곧 도입할 것으로 예상됩니다.[14]

공공 부문은 디지털 위험에 대한 인식 제고 측면에서 민간 부문보다 훨씬 앞설 뿐만 아니라, 임무의 성공을 위한 디지털 위험 요소의 진단, 우선 순위 지정 및 처리 측면에서도 많은 진전을 보이고 있습니다.

결론

오늘날의 정부 조직은 주민에게 서비스를 제공하고 임무 성과를 높일 수 있는 기술적인 방법을 지속적으로 현대화하고 있습니다. RSA 디지털 위험 연구에서 명확히 알 수 있듯이, 디지털 혁신과 관련된 위험을 관리하는 것이 정부 보안 책임자의 최우선 과제입니다. 하지만 디지털 혁신이 점점 더 오늘날 정부의 업무를 규정함에 따라 디지털 위험도 점점 더 커지고 있습니다. 이러한 위험은 여기에서 논의된 세 가지 위험에 국한되지 않습니다. 기관의 임무에 영향을 미치는 규제 위험, 운영 위험 등도 포함됩니다. 이러한 위험은 분명히 정부에 더 큰 부담이 되며, 당면 과제도 늘어납니다. 하지만 의심의 여지가 없는 한 가지는 디지털 혁신에 관한 위험 관리의 필요성입니다. RSA 디지털 위험 연구에 따르면, 디지털 혁신이 이루어지고 있는 공공 부문의 조직은 이에 대해 매우 잘 알고 있습니다. 이러한 사실은 디지털 위험에 대한 인식 제고 측면에서 공공 부문이 민간 부문보다 훨씬 앞설 뿐만 아니라, 임무의 성공을 위한 디지털 위험 요소의 진단, 우선 순위 지정 및 처리 측면에서도 많은 진전을 보인다는 사실을 나타냅니다.

디지털 위험은 모두에게 중요한 과제이며

이 위험을 관리하도록 지원하는 것은 RSA의 몫입니다

RSA® Business-Driven Security™ 솔루션은 통합된 가시성, 자동화된 분석 정보 및 조율된 작업에 따라 디지털 위험을 관리하는 통합된 접근 방식을 조직에 제공합니다. RSA 고객은 신속한 감지 및 대응, 사용자 액세스 제어, 소비자 부정 행위 방지 및 통합 위험 관리를 위한 솔루션을 통해 혁신적인 변화를 추진하고 이러한 변화에 지속적으로 적응할 수 있습니다.

rsa.com/ko-kr에서 역동적이고 위험도 높은 디지털 세상에서 성공하는 방법에 대해 알아보시기 바랍니다.

1 "Information Technology Management Reform Act of 1996", Wikipedia: 무료 백과사전, Wikimedia Foundation, Inc., 2019년 2월 19일 오후 7시 45분, https://en.wikipedia.org/wiki/Information_Technology_Management_Reform_Act_of_1996(2019년 10월 10일에 액세스함)

2 "E-Government Act of 2002", Wikipedia: 무료 백과사전, Wikimedia Foundation, Inc., 2019년 4월 18일 오후 2시, https://en.wikipedia.org/wiki/E-Government_Act_of_2002(2019년 10월 10일에 액세스함)

3 "OMB announces 'cloud first' policy for agencies", Federal News Network, https://www.federalnewsnetwork.com/technology-main/2010/11/omb-announces-lsquocloud-firstrsquo-policy-for-agencies/(2010년 11월 23일)

4 "From Cloud First to Cloud Smart", 연방 클라우드 컴퓨팅 전략, https://cloud.cio.gov(2019년 10월 10일에 액세스)

5 "Federal Information Security Modernization Act of 2014: Annual Report to Congress", https://www.whitehouse.gov/wp-content/uploads/2019/08/FISMA-2018-Report-FINAL-to-post.pdf(2018 회계연도)

6 "Key Issues: Cybersecurity Challenges Facing the Nation—High Risk Issue", 미 회계감사원, https://www.gao.gov/key_issues/ensuring_security_federal_information_systems/issue_summary(2019년 10월 10일에 액세스함)

7 "High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas", 미 회계감사원, https://www.gao.gov/products/GAO-19-157sp#summary(2019년 3월 6일)

8 "22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault", National Public Radio, https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault(2019년 8월 20일)

9 Allen Kim, "In the last 10 months, 140 local governments, police stations and hospitals have been held hostage by ransomware attacks", CNN, https://www.cnn.com/2019/10/08/business/ransomware-attacks-trnd/index.html(2019년 10월 8일)

10 "Cyberdefense for Texas State Government", 회계 문서: A Review of the Texas Economy, 텍사스주 감사원장 Glenn Hegar 집무실에서 제공, https://comptroller.texas.gov/economy/fiscal-notes/2019/mar/tx-cyberdefense.php (March 2019)

11 "2019 Data Breach Investigations Report", Verizon, https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf(2019년 5월)

12 Kristin Ann Shepard, "Data Privacy Exposure Hits the Public Sector", The National Law Review, https://www.natlawreview.com/article/data-privacy-exposure-hits-public-sector-lessons-opm-data-breach-class-action(2019년 8월 13일)

13 "What are we doing to protect taxpayer privacy?" IRS, https://www.irs.gov/privacy-disclosure/what-are-we-doing-to-protect-taxpayer-privacy(2019년 10월 18일)

14 Alex Hickey, "Government takes baby steps in data privacy with NIST framework, bill discussions," CIO Dive, https://www.ciodive.com/news/government-takes-baby-steps-in-data-privacy-with-nist-framework-bill-discu-1/550084/(2019년 3월 12일)

15 "RSA 디지털 위험 연구", RSA 디지털 위험 보고서, 초판본, https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf(2019년 9월)