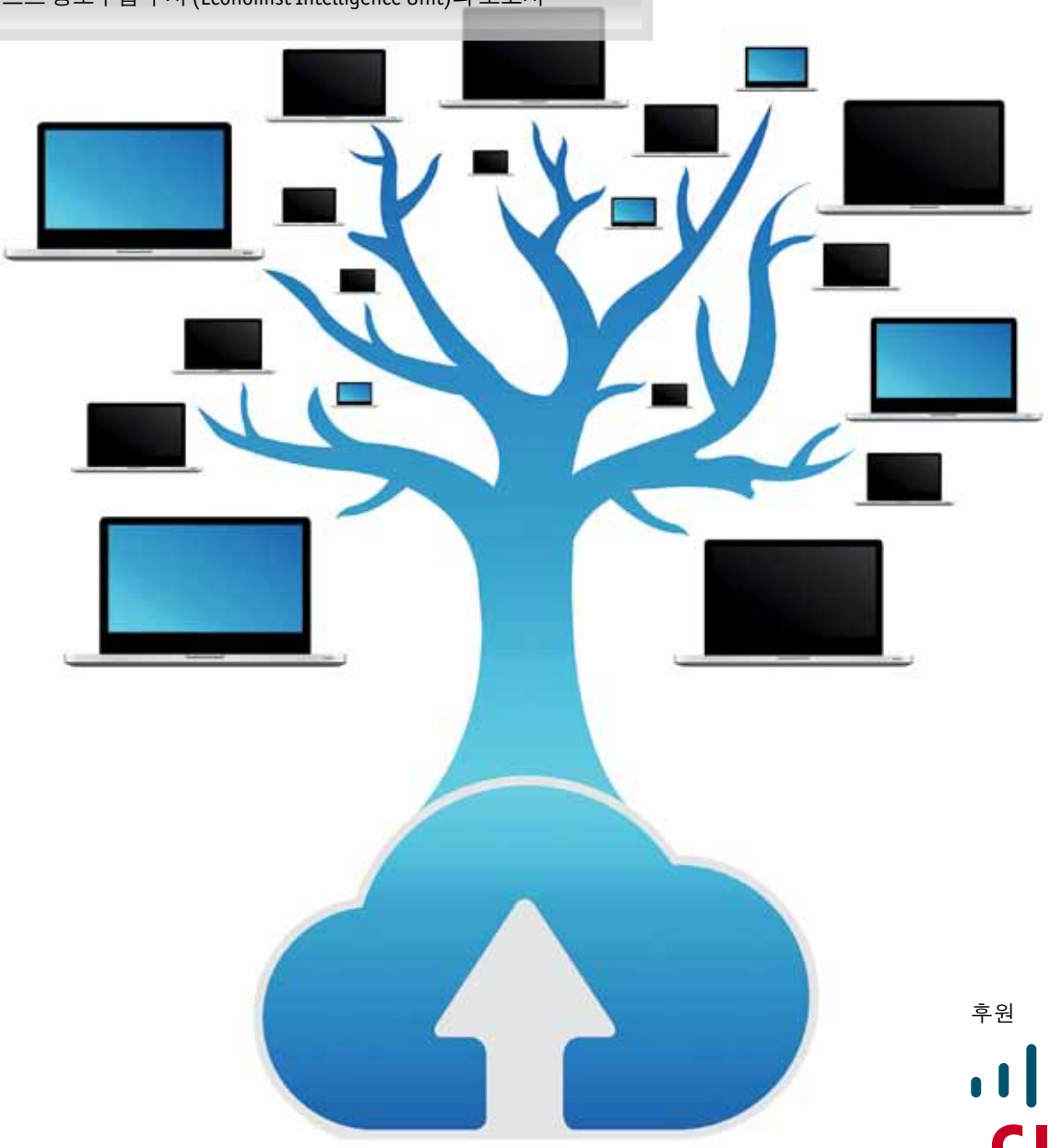
Economist Intelligence Unit

The Economist

모바일 세상에서의 안전한 데이터 액세스

이코노미스트 정보수집 부서 (Economist Intelligence Unit)의 보고서



후원

CISCO

목차

서론

기업들은 직장 내에서의 개인용 통신기기의 사용이 증대되고, 이동 중의 임원 및 직원들의 생산성을 극대화 할 필요성이 대두되고 있는 상황에 대처해야 한다. *"모바일 세상에서의 안전한 데이터 접속"* 은 기업들이 비즈니스 정보를 모바일로 접속하고자 하는 증대되는 수요에 어떻게 부응해야 하고, 독점 자료에 대한 보안 리스크를 최소화할 수 있는 방법에 대해 살펴보았다. 본 보고서를 위해, 이코노미스트 연구소는 2012년 6월 전세계 578명의 최고 임원들을 상대로 설문조사를 실시하였다. 본 설문조사는 BYOD (Bring Your Own Device, 회사가 직원들에게 업무용으로 개인의 스마트폰과 태블릿을 사용하도록 허용하는)와 더욱 더 일상화되고 있는 직원들의 이동성이라는 멈출 수 없는 최근의 움직임으로 인해 현재 또는 앞으로 생겨날 도전과제에 대해 조직들이 어떻게 대응해야 할지를 살펴보았다. 일련의 심층 인터뷰 또한 진행되었다. 본 보고서의 분석결과와 견해는 후원사의 입장을 반영하고 있지 않다. 본 보고서의 저자는 린 그레이너 (Lynn Greiner)이다. 편집자는 마이클 싱어 (Michael Singer)와 저스틴 쏘디 (Justine Thody) 였으며, 지면 배정은 마이크 케니(Mike Kenny)가 담당하였다. 익명으로 통찰력있는 견해를 제공해준 분들을 포함하여 본 설문조사와 인터뷰를 위해 귀중한 시간을 내어 의견을 내어주신 모든 임원분들께 감사를 전한다.

인터뷰 대상자

루시 버로우 (Lucy Burrow), 킹스 칼리지 런던 (King's College, London)의 IT 거버넌스 책임자

마이크 코디 (Mike Cordy), 오앤엑스 엔터프라이즈 솔루션 (OnX Enterprise Solutions) 글로벌 최고 기술 책임자

스티브 엘리스 (Steve Ellis), 웰스파고은행 (Wells Fargo) 수석 부행장

제이 리크 (Jay Leek), 블랙스톤그룹 (Blackstone Group) 최고 정보보안 책임자

알투로 메디나 (Arturo Medina), 입소스 맥시코 (Ipsos Mexico) 정보기술 책임자,

빌 머피 (Bill Murphy), 블랙스톤그룹 (Blackstone Group) 최고 기술 책임자

알 레이몬드 (Al Raymond), 아라마크 (Aramark) 부사장

아쉬와니 티쿠 (Ashwani Tikoo), CSC 인도 최고 정보 책임자

요약

1990년대 후반, 휴대용 노트북과 모바일 기기의 등장은 경영진들에게 사무실 밖에서도 생산적으로 일할 수 있는 환경을 제공하였다. 아이비엠 (IBM)사의 씽크패드 (ThinkPad)와 림 (RIM)사의 블랙베리 (BlackBerry)와 같은 기기의 등장으로 다기능을 탑재한 모바일 기기의 시대가 도래하게 되었으며, 이는 임원들에게 있어 거부하기 어려운 움직임이었다. 오늘 날, 모바일을 사용하는 전세계 근로자 수는 사무실 공간에 비해 훨씬 많으며, 2015년까지 모바일 근로자 수는 13억명 또는 전체 근로자의 13%가 될 것이라고 테크놀로지 리서치 업체인 IDC는 전망했다. 어떤 이들은 기업의 최대 76%가 BYOD (Bring Your Own Device, 회사가 직원들에게 업무용으로 개인의 스마트폰과 태블릿을 사용하도록 허용하는) 정책을 옹호하고 있으며, 이는 회사가 소유하지 않은 기기를 통한 데이터 접속을 보장해줘야 하는 결과를 초래하였다고 말한다. 이들 기업의 대부분은 직원들이 더 효과적이고, 협력적인 결정을 하고, 기회를 놓치는 경우가 줄이며, 파트너와 고객과 효과적으로 일할 수 있게 하기 위해 개인용 기기의 사용을 허용하고 있다고 말하며, 이는 회사 소유의 기기를 통한 모바일 데이터 접속을 허용하는 이유와 동일하다.

2012년 6월 이코노미스트 연구소는 시스코 (Cisco) 사의 후원으로 전세계 578명의 임원을 대상으로 설문조사를 실시하여, 모바일 기기를 통해 접속하는 데이터 보호에 대한 이들의 견해를 구하고자 하였다. 설문조사의 결과는 다음과 같았다.

- **대부분의 임원들은 회사 데이터에 대한 모바일 접속 정책에 대해 불안해 하고 있었다.** 응답자의 42%가 경영진이 가장 생산적이기 위해 전략기획 자료에 안전하고,

설문조사에 참여한 응답자들은 어떤 이들인가?

본 설문조사는 전세계 578명의 임원들을 대상으로 실시되었다. 설문조사 응답자의 대다수는 북미 지역 (29%), 서유럽 (25%), 아시아 태평양 지역 (27%)에 주재하고 있었으며, 나머지 임원들은 중동과 아프리카, 남미, 동유럽에서 근무하고 있었다. 전체 응답자 중 23%는 미국, 10%는 인도, 7%는 캐나다, 6%는 영국 출신이었다. 직책을 살펴보면, 최고 경영자가 27%, 수석 부사장은 17% 그리고 중간 관리자급은 15%였다. 조직 규모의 경우, 55%는 연간 매출 미화 5억 달러 이상, 22%는 미화 100억 달러 이상이었다. 응답자들은 다양한 업계를 대표하고 있었으며, 특히 IT와 기술 분야 13%, 금융 서비스 11%, 전문직 서비스 11% 그리고 에너지와 천연 자원은 9%를 차지했다. 직무에 대해 응답자들은 일반 관리, 사업 개발, 재무 그리고 영업. 마케팅을 담당한다고 응답했다. ■

시의 적절하게 접속할 필요가 있다고 대답하였으나, 모바일 기기를 통해 이러한 데이터에 접속하는 것이 적절하다고 생각한 응답자는 28%에 불과했다. 거의 절반에 가까운 응답자의 49%는 여러 데이터 소스를 보호하는 복잡성 그리고 응답자의 48%는 모바일 접속에 대한 지식 부재와 리스크를 기업이 당면한 가장 큰 도전과제라고 응답했다.

- **대규모 기업은 중요 데이터에 대한 모바일 접속을 허용할 의사가 가장 크나, 이와 동시에, 보다 엄격한 제한을 적용하였다.** 매출이 미화 10억 달러 이상인 기업의 90% 이상이 개인용 또는 회사 소유의 기기를 통한 접속을 허용하고 있었다. 그러나, 매출이 미화 5억 달러 이상인 기업의 경우, 50% 이상은 회사 소유의 기기를 통한 접속을 허용하고 있었고, 1/3은 개인용 기기를 통한 접속을 허용하고 있었다. 이와 대조적으로, 매출이 미화 5억 달러 미만인 기업의 경우, 37%만이 회사 소유의 기기를 통한 접속을 고집했고, 47%는 개인용 기기를 통한 접속을 허용하고 있었다. 그러나, 규모가 큰 기업의 모바일 사용자 일수록, 다단계 정책 승인을 거친 허가된 기기만을 사용할 수 있었다.

- **모바일 정책은 소셜 네트워킹을 다루지 않을 수 없다.** 설문조사 응답자의 56%가 모바일 기기를 통한 소셜 네트워크의 허용범위를 규정하는 정책을 가지고 있다고 답한 반면, 응답자의 33%는 소셜 미디어 플랫폼 상에서 업무 관련 이야기를 하는 것이 금지되어 있다고 대답했다. 소셜 네트워킹에 대한 정책을 신중히 따른다면, 효과적인 상호작용을 하면서, 기업의 데이터 자산을 보호하고, 법적 분쟁을 피할 수 있을 것이다.

- **모바일 액세스에 대한 회사 정책에 가장 큰 영향을 미치는 요소 중 하나가 사용 가능한 인프라이다.** 응답자의 44%가 정책에 영향을 미치는 가장 중요한 요소가 임원들의 압력이라고 대답하였으나, 이 수치는 IT 인프라 요건이라고 대답한 60%의 응답률에 밀렸다. 이는 모바일 접속을 보호하고 관리하는 서비스를 제공하는 기업들에 있어 기회가 존재함을 시사한다.

모바일 데이터 액세스는 멈출 수 없는 움직임인가? 결론적으로 "그렇다" 라고 답할 수 있으며, 더 나은 사용자 경험을 제공하기 위해 더욱 정교해진 기기는 이러한 변화를 더욱 가속화시킬 것이다. 이것이 의미하는 바는 관련 정책을 수립하는 일이 선택사항이 아닌 의무사항이라는 것이다. 본 설문조사에 응한 임원들은 직원 참여를 통해 모바일 관련 정책을 수립함으로써 정책의 준수 가능성을 높일 수 있다라고 말했다. ■

서론

많은 기업에 있어, 모바일 데이터 접속에 관한 올바른 정책을 채택하는 일은 점점 더 고민거리가 되고 있다. 젊은 직원들 못지않게 임원들도 모바일 기기 뿐 아니라 특정 장소에 고정된 기기를 통해 기업자료를 언제 어디에서든 접속하고 싶어한다. 많은 기업들이 모바일 기기 정책을 옹호함으로써 근무 외 시간에 직원들이 업무에 대한 응대를 하는 등의 근무의지를 높이고, 직원 참여도와 생산성을 제고할 수 있음을 깨닫고 있다. BYOD에 친화적인 근무환경은 혁신을 촉진하는데 도움이 되는 기술동향에 민감한 직원을 유치하는데도 도움이 된다.

모바일 기기가 급증하고, 개인 및 업무용 IT 간의 구분이 모호해짐에 따라, 기업들이 당면한 과제는 어떻게 이러한 문화적인 변화를 수용하느냐이다. 접속할 수 있는 비즈니스 데이터의 확대는 응당 비즈니스 리스크 뿐 아니라, 기술적 도전과제를 수반한다. 휴대용 기기는 분실하거나 도난 당할 수 있다. 사람들은 친구나 친지들과 기기를 공유할 수 있으며, 이는 기밀 정보의 유출이라는 위험을 증대시킨다. 종종 회사에서 허가하지 않은 소프트웨어 애플리케이션을 통해 이러한 데이터에 접속하는 경우도 있다. 하지만, IT 부서가 직원들이 직장에 가져오는 개인용 기기나 사무실 밖에서 사용하는 기기에 대해 통제하는 일은 점점 더 무의미해지고 있다. 이들은 회사 데이터 네트워크가 수반하고 있는 증대되는 취약성에 대한 대비를 해야 한다. 이는 업무상 중요한 자료를 보호하면서도 기업이 운영하고 있는 모든 지역의 규제환경에 부합할 수 있는 효과적인 보호장치의 설치를 통해 가능하다. ■

1 현대의 이동성: 현재 우리 모습은?

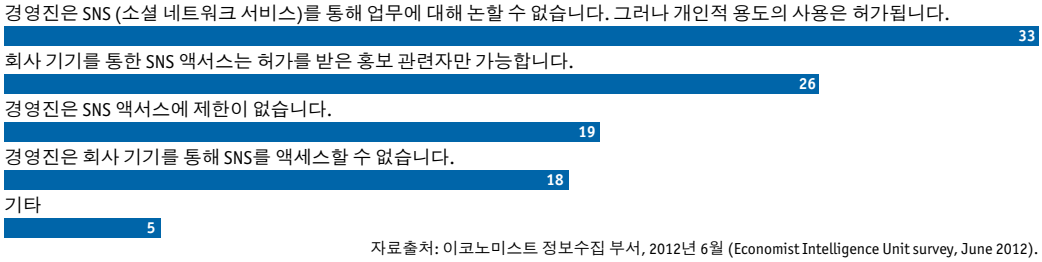
기술 리서치 기관인 IDC는, 2011년 한해 전세계에 판매된 스마트 기기는 10억대에 달하며, 2016년까지 이 수치는 2배가 될 것이라고 전망했다. 이들 기기는 노트북, 넷북, 휴대폰 그리고 태블릿과 같은 PC 기반 제품이 포함하고 있다. 이코노미스트 연구소의 설문조사에 따르면,대다수의 사람들이 여러 대의 기기를 동시에 사용하고 있었으며, 가장 흔히 노트북과 스마트폰을 함께 사용하였으며, 태블릿은 그 이용이 점차 늘어나고 있는 것으로 확인되었다. IDC의 보고에 따르면, 2012년 2분기 동안 전세계 태블릿 판매량은 1분기 대비 33.6% 증가했으며, 전년 동기대비, 66.2% 성장했다. 본 연구소는 차세대 소프트웨어 운영 시스템이 출시된 후, 태블릿의 사용이 폭발적으로 증가할 것으로 예상한다. 새로이 출시되는 태블릿에 협업기능과 통신기능이 추가된다면, 임원들은 스마트폰 보다 더 광범위해진 데이터 접속 방법을 제공하는 태블릿을 선호하게 될 것이다.

IT 서비스 제공업체인 CSC 인도의 최고 기술 책임자인 아쉬와니 티쿠 (Ashwani Tikoo)는 이동 중의 임원들에게 모바일 기기를 통해 정보를 제공하게 되면, 비즈니스 협상과 같이 중요한 시점에 이들이 빠르고, 현명한 의사결정을 내리는데 도움이 될 것이다라고 말한다. CSC 글로벌의 두 번째로 규모가 큰 운영센터에서 최고기술책임자인 티쿠(Tikoo)는 모바일 기기 상의 기업 데이터를 보호하는 보안정책에 대한 책임을 맡고 있다. 데이터를 즉각적으로 제공받게 됨에 따라, 영업직원들은 고객을 기다리게 하지 않고, 현장에서 바로 올바른 의사결정을 할 수 있게 될 것이라고 그는 말한다. 데이터 손실을 방지하기 위해, CSC의 보안 정책은 BYOD 정책 하에 허용되는 개인용 기기를 포함한 모든 모바일 기기에서의 데이터 암호화를 의무화하고 있다.

모바일 기기 상에 데이터를 저장하지 못하도록 하는 것 또한 여러 보안 전략 중 하나다. 미국 식품서비스 공급업체인 아라마크 (Aramark)사의 알 레이몬드 (Al Raymond) 프라이버시 및 기록 관리 담당 부사장은 회사 정보에 원격으로 접속할 필요가 있는 승인된 사용자는 자신의 노트북이나 모바일 기기를 통해 가상사설망 (Virtual Private Network, VPN)에 접속하여 해당 정보에 접속할 수 있다고 말한다.

Q 경영진 모바일 소셜 정책

회사 장치를 통한 SNS 액세스와 관련 귀사는 어떤 규정을 운영하고 계십니까?
(응답자 비율 %)



자료출처: 이코노미스트 정보수집 부서, 2012년 6월 (Economist Intelligence Unit survey, June 2012).

사례 연구: 하이브리드식 접근방법을 채택한 입소스 (Ipsos)

시장 조사를 진행함에 있어 일대일 접촉을 선호하는 남미와 같은 지역에서 스마트폰과 태블릿은 연필과 종이와 같은 설문조사 도구를 대체하고 있다. 글로벌 시장조사 업체인 입소스 (Ipsos)는 모바일 기기를 사용하는 이러한 움직임을 적극 수용하여 멕시코와 기타 지역에서의 사업을 운영하기 시작했다. 이 기업은 현재 84개 국가에서 운영되고 있으며, 약 16,000명에 달하는 정규직 직원을 보유하고 있다. 시장조사에 사용되는 조사 방법 또한 온라인에서부터 면대면 조사에 이르기까지 다양하여, 매년 전세계에서 진행하는 인터뷰수가 7천만 건에 달하고 있다.

입소스 (Ipsos)는 현재 회사 소유의 휴대용 기기를 인터뷰 담당자에게 제공하고 있으나, 새로운 접근방법을 개발 중에 있다고 입소스 멕시코 (Ipsos Mexico) 정보기술 책임자인 알투로 메디나 (Arturo Medina)는 말한다. "맞춤형 모바일 기기 비용이 상당히 비싸기 때문에 BYOD 정책의 하이브리드 모델을 채택하고 있다"고 그는 말한다.

현재 개발 중인 하이브리드 모델하에서, 인터뷰 담당자들은 입소스 (Ipsos)사의 인터뷰 소프트웨어를 실행 가능한 것으로 확인된 스마트폰 모델 3가지 중 하나를 선택할 수 있다. 직원들은 기기에 대한 대금을 점진적으로 급여에서 차감하는 방식으로 지불한다. 보통, 기기를 소유하게 되기까지 2-3주 정도가 소요된다고 메디나 (Medina) 정보기술 책임자는 말한다.

입소스 (Ipsos)는 기업 데이터에 접속할 수 있도록 VPN 연결을 제공하며, 직원들은 나머지 스마트폰 기능 이용에 대한 비용을 부담한다. 입소스 (Ipsos)는 필요한 경우, 원격으로 업무 정보를 삭제할 수 있도록 기기를 관리한다. 스마트폰에서 접속한 정보는 암호화가 되어 있어 데이터의 손실을 방지할 수 있다. 인터뷰 담당 직원들은 또한 회사의 이용정책을 준수해야만 한다. 인터뷰 담당자들은 하나의 기기를 어디에서나 사용할 수 있는 융통성을 가지게 되며, 회사는 데이터 자산을 보호할 수 있는 충분한 통제력을 갖게 된다고 메디나 (Medina) 정보기술 책임자는 말한다. ■

이메일 이외의 다른 데이터는 기기상에 저장되어 있지 않으며, 이는 직원이 퇴사하거나 기기를 분실할 경우에도 상대적으로 쉽게 기업 데이터를 보호할 수 있게 한다.

회사 정책 상 임원들의 소셜네트워킹 행동은 제한되고 있긴하나, 사무실 밖에서 모바일 기기를 통해 소셜 네트워킹에 참여하는 행위 또한 비슷한 도전과제를 수반한다. 이코노미스트 연구소의 설문조사에 참여한 임원 응답자의 33%가 소셜 네트워크상에서 업무 관련된 내용에 대해 언급할 수 없다고 답했으며, 1/4은 승인된 대변인만이 회사 기기를 통해 소셜 네트워크에 접속할 수 있다고 대답했다. 본 연구소의 설문조사 결과, 기업 정보를 보호하고 법적 분쟁을 피하기 위해, 명문화된 정책을 통해서든 암묵적인 합의를 통해서든 임원들의 소셜 네트워킹 활동은 계속해서 제한될 것으로 보인다.

물론, 조직 내에서의 위치에 따라 접속할 수 있는 데이터의 유형도 달라져야 하는데, 본 연구소의 설문조사에서 몇 가지 놀라운 사례가 발견되었다. 임원들에게 있어 생산성을 재고하는데 중요한 정보는 재무관련 정보가 60%, 전략기획 정보가 42%였다. 중간 관리자에게 있어 중요한 정보는 운영정보가 44%, 영업 및 마케팅 정보가 43%였으며, 일반 직원들에게 가장 필요한 정보는 고객정보와 운영정보로 각각 42%를 차지했다. 본 연구소의 조사결과, 임원들이 중요한 비즈니스 데이터에 대한 모바일 액세스가 필요한 가장 중요한 이유로 효과적인 의사결정 (52%)과 사업기회를 놓치지 않기 위해(42%)가 꼽혔다. 소규모 기업이 모바일 접속이 필요한 가장 주된 이유는 공급업체와 같은 제3자와의 커뮤니케이션을 위해서였다. 본 설문조사에 참여한 모든 기업의 37%가 모바일 접속이 필요하다고 답한 반면, 매출이 미화 5억불 이하인 기업 응답자의 42%가 이를 모바일 접속이 필요한 주된 3가지 이유 중 하나로 뽑았다. 인터넷 접속의 필요성으로 인해 이메일은 모바일 기기에 반드시 탑재해야 하는 필수 어플리케이션이 되었다. 본 설문조사에 참여한 임원들 (81%)에게 있어 이메일은 비즈니스 데이터를 원격으로 접속하는데 사용되는 가장 주된 툴이라고 답했다. ■

2 데이터 손실, 유출 및 나쁜 관행: 이러한 도전과제를 극복하기 위한 기업들의 조치는?

다양한 플랫폼을 통해 기업 데이터를 안전하게 접속하기 위한 시스템 구현에는 비용이 든다. 이런 측면에서, 설문조사에 참여한 대규모 회사의 응답자들이 자신이 근무하는 회사의 데이터 보안 상황에 대해 자신감을 가지는 일은 당연하다. 연간 매출이 미화 100억 달러 이상인 기업의 응답자의 45%가 그들의 기업이 최첨단 데이터 보안 조치를 마련하고 있다고 응답한 반면, 같은 응답을 한 소규모 기업 (연간 매출 미화 5억 달러)의 응답자는 고작 10%에 불과했다. 또한, 연 매출이 미화 5억에서 50억 달러 사이의 기업에 종사하는 응답자의 무려 1/3이 그들의 보안정책이 부적절 또는 매우 부적절하다고 응답하였다.

전반적으로, 설문조사에 참여한 임원 응답자의 69%가 보안 서비스에 대한 투자를 우선순위로 꼽으며, 투자가 필요하다는 사실을 인지하고 있었다. 그러나, 본 연구소의 설문조사 결과는 임원들에게 보안 리스크에 대한 교육을 실시할 필요가 있음을 시사했다. 공고한 보안수준을 유지하고 있다고 믿는 일부 기업들의 경우, 위험한 관행을 허용하고 있었다. 일례로, 자신들이 근무하는 회사가 업계 최고의 보안 관행을 가지고 있다고 대답한 20%의 응답자 중 13%가 그들의 소셜 네트워킹 활동에는 제한을 받지 않고 있다고 답변했다. 이러한 관행은 물론, 회사 기밀 정보를 실수로 공개하는 위험을 수반한다. 본 연구소의 조사결과는 소셜 네트워킹에 대한 정책 수립이 효과적인 대인관계를 유지하면서, 기업 데이터 자산을 보호하고, 법적 분쟁을 피하게 하는 결과를 가져옴을 보여주었다.

대기업보다 자원이 부족한 소기업은 모바일 데이터 보안에 있어 더욱 도전적인 과제에 당면해 있다. 연간 매출이 미화 5억 달러 미만인 기업의 응답자의 약 40%가 그들 회사의 모바일 데이터 보안 정책이 부적절 또는 매우 부적절하다고 대답했다. 대기업과 마찬가지로 소규모 기업들도 문서화된 정책을 이행함으로써 상대적으로 저렴한 비용으로 기업 데이터를 보호할 수 있다. 지난 몇 년간 판매된 모바일 기기들은 암호화기능을 내장하고 있어 활성화만 하면 된다. 그러나, 보안 절차를 자동화하기 위해서는 흔히 추가적인 관리 툴이 필요한데, 이는 소규모 기업들로 하여금 데이터 보안 기술을 구입하는 방법과 직원들에게 보안 정책 준수의 책임을 묻는 등의 낮은 비용을 수반하는 방법 간에 저울질을 하게 만들었다.

크기가 아주 작은 모바일 기기이더라도 그 영향력이 커짐에 따라 비기술적인 사유로 데이터를 상실할 위험 또한 커지고 있다. 미국 기반의 컴퓨터 노트북 주변기기 제조업체인 켄싱턴사 (Kensington)에 따르면, 매년 7천만 대 이상의 스마트폰이 분실되고 있으며, 이 중 단 7%만이 반환되고 있다고 한다. 노트북도 예외는 아니다. 켄싱턴사 (Kensington)의 연구 결과에 따르면 개인용 컴퓨터 (PC)의 10%가 총 제품 수명 기간 동안 분실 또는 도난 된다고 한다. 분실의 3/4는 출퇴근하면서 또는 사무실 이외의 장소에서 근무하는 동안 발생된다고 한다. 이렇게 분실된 대다수의 컴퓨터는 일종의 비즈니스 데이터를 저장하고 있다.

컨설팅 업체인 포네몬 연구소 (Ponemon Institute) 에 따르면, 데이터 유출 사고로 인해 기업이 부담하는 평균 비용은 2010년 미화 720

BYOD 이해하기

BYOD 모델이 상대적으로 새로운 개념이기 때문에, BYOD 정책에 대한 검증된 업계 표준이 존재하지 않는다. 일반적으로, 직원이 자발적이든 타의에 의해서든 퇴사하게 되면, 직원의 개인정보에 영향을 주지 않으면서, 기업 데이터는 재빨리 삭제할 필요가 있다. 이와 관련된 조항은 BYOD를 위해 허용되는 여러 정책 중 하나이다. 기업들은 또한 기존의 모바일 정책을 개정함으로써 법적 보호를 받을 수 있다고 2012년 6월호 국가법률저널 (National Law Review)는 권장한다. 성희롱, 성차별, 고용평등 관련 정책, 기밀유지 및 보호에 관한 정책 그리고, 기업준수 및 윤리강령에 대한 정책들 모두 근로자에 의한 모바일 정책의 남용을 막기 위해 개정될 수 있다.

임원들의 위험한 관행을 최소화하기 위해 많은 기업들은 모바일 기기에 소프트웨어를 설치하여, 이들이 사용하는소프트웨어를 제재하고, 데이터는 암호화하며, 일정 업데이트 또는 보안 업데이트를 실행하는 등 기타 행정적 업무를 처리하고 있다. 사생활 침해로 느끼는 직원이 있을 수 있겠지만, 대부분의 모바일 기기 관련 정책들은 업무용 접속을 원격으로 통제하는 것을 허용한다. BYOD 정책을 가진 일부 기업의 경우, 임직원이 기기에필요한 소프트웨어를 자비로 설치하도록 규정하고 있다. 업무상 꼭 필요한 프로그램 비용을 전체 부담하거나 일부를 환급해 주는 기업들도 있다. 적절한 구성과 올바른 사용을 위해서는 중앙에서 이를 모니터링하고 이행해야 하며, 정기적인 보안관련 교육은 직원들 마음속에 안전한 데이터 접속에 대한 생각을 상기시켜 줄 것이라고 아라마크 (Aramarks)의 레이몬드 (Raymond) 부사장은 첨언한다.

레이몬드 (Raymond) 부사장은 기기 중심적인 모바일 보안 정책과 다른 접근방법을 취하고 있다고 말한다. 직원들은 모바일 기기를 통해 문서 보기만을 하고, 회사 데이터는 안전하게 접속가능하고, 과중한 계산을 수행할 수 있는 회사 서버에 보관하는 방식이 바로 그것이다. 안전한 네트워크로의 모바일 접속을 허용하는 방법에는 여러 가지가 있는데, 여기에는 가상 데스크탑 기술과 Salesforce.com과 같은 웹 기반의 서비스를 통한 데이터 접속등이 포함된다. 이러한 방법들은 기업에게 암호화, 인증 및 관리에 대한 통제를 가능케 하기 때문에 일반화되고 있다.

이와 유사한 네트워크 기반의 통제시스템을 관장하고 있는 입소스 (Ipsos)의 알투로 메디나 (Arturo Medina) 정보기술 책임자는 관련 정책을 준수하고, 기업데이터의 무단 다운로드를 방지하기 위해 직원들에게 이에 대한 교육을 지속적으로 실시할 것을 권고한다. M "민감한 정보와 사용자 개인 정보를 구분하고, 기업 정보로 백업할 것과 개인 정보로 간주할 것은 무엇인지 분명하게 구분해 두어야 한다." 라고 메디나 (Arturo Medina) 정보기술 책임자는 말한다. ■

Q BYOD 정책

귀사는 중요 데이터 액세스를 위한 BYOD를 어떻게 시현했습니까? 해당 항목을 모두 선택하십시오. (응답자 비율 %)

자료출처: 이코노미스트 정보수집 부서, 2012년 6월 (Economist Intelligence Unit survey, June 2012).

만불에 달한다고 한다. 이는 2005년에 기록된 평균 비용의 두 배에 달하는 수준이다. 데이터 유출 유형 및 건수를 고려할 때 이는 현실적인 수치라고 아라마크 사(Aramark)의 레이몬드 (Raymond) 부사장은 말하며, 매년 크고 작게 발생하는 수백만 건의 데이터 유출사고 규모는 2500만불에서 5억불에 이른다고 첨언했다.

직원들에 의한 데이터 유출을 방지하고자 하는 기업들은 대다수의 모바일 데이터 분실을 직접적으로 초래하는 사용자 부주의에 중점을 둔다. 포네몬 연구소 (Ponemon)의 *2011년도 데이터 유출 비용에 대한 연구 (2011 Cost of Data Breach)*에 따르면, 30~40%의 데이터 유출은 부주의로 인한 것이었으며, 43%는 악의적인 공격으로 인한 것이었다.. 본 연구는 또한, 이탈리아 기업의 데이터 유출의 50%가 모바일 기기의 손실 또는 도난 때문이라고 밝혔다. 독일 (42%), 프랑스 (43%) 및 호주 (36%)에서만이 부주의 보다 악의적인 공격으로 인한 데이터 유출이 더 많이 발생했다. 인도만이

유일하게 부주의 및 악의적인 의도 보다 기술적 결함으로 인한 데이터 유출 사고를 더 많이 경험하였다.

몇몇 건의 주목할 만한 모바일 데이터 유출 사고를 통해 유출사고가 얼마나 손쉽게 발생하는지 잘 알 수 있다. 인디애나폴리스 주재의 암 전문 클리닉인 암 관리 그룹 (Cancer Care Group)은 2012년 7월 서버 백업 파일을 저장한 직원의 노트북이 잠금상태의 차량에서 도난 되면서, 5만5천명 이상의 환자 및 직원의 개인정보가 유출되는 사고를 경험했다. 데이터 보안이 잘 되어 있는 모범 사례에서 볼 수 있는 것과 대조적으로, 이 경우 데이터는 암호화되어 있지 않았다. 텍사스에 위치한 의료센터인 MD 앤더슨 암센터 (MD Anderson Cancer Center)는 2012년 6월과 7월 사이 두 건의 유출사고를 경험하여 피해를 입었다. 이 중 한 건은 암호화되지 않은 휴대용 USB 키를 버스에서 분실하면서 발생했고, 또 다른 한 건 마찬가지로 암호화되지 않은 상태의 노트북이 직원의 집에서 도난되면서 발생했다. 이 두 건의 유출사고로 인해 3만명의 환자 개인정보가 유출되었다. 두 번째의 유출 사고 이후, 센터는 모든 데이터를 암호화하는 프로젝트에 착수했다.

기업들은 모바일 기기, 노트북, 스마트폰 또는 휴대용 데이터 저장 기기 등을 암호화를 통한 보호 기능을 추가하거나, 디스크나 USB 키를 전면 암호화하여 데이터 유출을 막을 수 있다.

이러한 장치에 대한 물리적인 보호장치 또한 필요하다. 일례로, 심지어 잠금 장치가 되어 있는 차량 안 이더라도 지켜보는 이가 없을 경우, 이들 기기를 남겨두어서는 안된다. (인텔사의 VPro 기술이 장착된) 휴대폰과 일부 PC 의 경우, 분실 시 원격으로 비활성화하여 데이터를 삭제할 수 있다. 암호는 언제든지 해제될 수 있으므로, 민감한 데이터가 저장되어 있을수록 이러한 보안 메커니즘을 준비해두는 것은 매우 중요하다. ■

3 모바일 데이터의 증가: 최신 동향

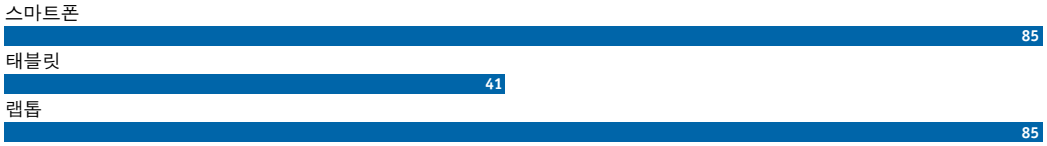
유럽연합 (UN) 산하기구인 국제전기통신연합 (International Telecommunication Union: ITU)에 따르면, 전세계 조직의 약 90%가 중요한 데이터에 대한 모바일 접속을 허용하고 있다. 본 연구소의 설문조사에서 공식적인 BYOD 정책을 구비하지 않고 있는 것으로 확인된 조직 중 25%가 향후 12-18개월 내에 관련 프로그램을 도입할 계획이라고 밝혔다. 한 독립적인 연구기관이 주장하고 있는 바에 따르면, 이러한 프로그램이 직원들에게 더 많은 동기부여를 한다고 한다. 미국의 모바일 소프트웨어 회사인 아이패스 (iPass)가 2012년 8월에 실시한 조사에 따르면, 항상 연결되어 있는 상당수의 직원들이 1주일에 최대 20시간은 무급으로 추가 근무를 하고 있는 것으로 조사되었다. 아이패스 (iPass) 사의 설문조사 응답자의 약 90%가 수도나 전기처럼 무선 연결성이 일상생활의 중요한 요소라고 답했다.

사무실 밖에서 근무하는 직원이 증가하고 있음에도, BYOD를 포함한 모바일 액세스 프로그램을 수립할 수 없는 기업들이 있다. 은행과 금융회사와 같이 엄격한 규제를 받는 기업의 경우, 개인 기기를 통한 회사 데이터 접근을 금지하는 엄격한 정책을 가지고 있다. 스티브 엘리스 (Steve Ellis) 웰스파고은행 (Wells Fargo) 수석 부행장은 당 은행이 BYOD에 대해 신중하게 접근하고 있으며, 현재 여러 가지 대안을 두고 고민 중이라고 말했다. 엘리스 수석부행장은 공식적인 계획이 수립될 때까지 앞으로 1년은 더 걸릴 것이라고 첨언했다. 공식적인 BYOD 정책이 없는 기업에서 직원들이 암암리에 개인 기기를 활용하는 사례들이 늘어나고 있다. 아라마크 사(Aramark) 가 공식적인 모바일 정책을 도입하기 10개월 전만 하더라도, 내부적으로 회사네트워크에 연결할 수 있는 기기와 운영시스템은 무엇인지 알려주는 명문화된 가이드라인이 없었다. 역할에 따른 액세스 권한부여와 연결 가능한 기기와 승인된 기기 및 구성에 대한 내용을 담은 새로운 정책이 도입됨에 따라, 아라마크 사 (Aramark)는 이제 누가 어떠한 데이터에 대한 액세스 권한을 가지는지 정확히 파악할 수 있게 되었다. "이제 (잘못된 줄 알면서도 묵인하는) 기존의 방식은 통하지 않는다." 라고 레이몬드 (Raymod) 부사장은 말한다. 프로그램이 더 가시화될수록 그만큼 이행 가능성도 높아진다.

정책 뿐 아니라 기기의 유형 또한 변화되고 있다. 본 연구소의 조사에 따르면, 스마트폰을

Q 임원 액세스 장치

귀사에서 임원의 중요 데이터 액세스를 위해 제공하는 장치는 무엇입니까?
해당 항목을 모두 선택하십시오.
(응답자 비율 %)



자료 출처: 이코노미스트 정보수집 부서 설문조사, 2012년 6월 (Economist Intelligence Unit survey, June 2012).

사례 연구: 미국평등고용위원회 (EEOC) , 이동성 시범사업 출범하다.

미국평등고용위원회 (Equal Employment Opportunity Commission, EEOC) 의 2012년 회계연도 예산은 미화 1760만 달러에서 1500만 달러로 거의 15%나 삭감되었다. 운영 경비를 줄여야 했던 최고정보 책임자 킴벌리 핸처 (Kimberly Hancher)는 모바일 기기 예산을 절반으로 줄였다. 예산 감축에 대응하기 위해, 위원회는 모바일 BYOD 시범 프로젝트에 착수하였다. 이 프로젝트의 목표는 직원들에게 위원회의 이메일, 일정표, 연락처 그리고 등록한 작업에 접속할 수 있는 권한을 제공하는 것이었다. 이 프로젝트의 일환으로 몇몇 고위 임원들에게는 위원회의 내부 시스템에 접속 할 수 있는 "특권" 이 주어졌다.

초기 검증 단계에서 40명의 지원자들은 정부가 제공한 블랙베리 (BlackBerry) 를 반납하고, 그 대신 개인 스마트폰을 사용하였다. 정보 보안 및 법률 부서의 직원들과 직원 조합은 미국 국립표준기술연구소 (National Institute of Standards and Technology, NIST)의 규정인 SP 800-53 ("연방 정보 시스템 및 조직을 위한 권장 보안 통제"라고도 함)처럼 직원의 개인 프라이버시 (소셜 미디어 및 모니터링 정책)와 정부 보안 간의 균형을 맞출 수 있는 규정을 만들어냈다. 이 프로그램의 두 번째 단계는 2012년 6월에 개시되었다. EEOC는 계약업체와의 협업을 통해 두 번째 시범프로그램에 참여하는 직원들에게 위원회의 이메일에 접속할 수 있는 권한을 제공하였다. EEOC가 제공한 블랙베리 (BlackBerry) 를 이용하는 나머지 468명의 직원들에게는 다음의 세 가지 선택권을 제공하였다.

1. 블랙베리 (BlackBerry)를 자발적으로 반납하고, 개인용 안드로이드, 애플 (Apple) 또는 블랙베리 (BlackBerry) 스마트폰 또는 태블릿을 직장으로 가져온다.

2. 블랙베리 (BlackBerry)를 반납하고, 음성 기능만 가능한 정부가 제공한 핸드폰을 수령한다.

3. EEOC에 대체 기기가 없음을 이해하고, 블랙베리 (BlackBerry)를 계속 사용한다.

현재까지 시범 프로그램에 대한 EEOC 중간관리자들의 반응은 긍정적이다. 직원들은 개인이 사용한 음성 및 데이터 사용에 대해 비용을 지불하고, 위원회는 소프트웨어 관리를 위한 라이센스 비용을 지급한다. EEOC의 핸처 (Hancher)는 일부 직원들에게 있어 비용이 문제가 될 수 있고, 직원이 사용한 데이터 및 음성 서비스의 일부에 대해서만 위원회가 비용을 환급해 줄 수 있을 지가 미해결 과제이다라고 말한다. 핸처 (Hancher) 는 직원, 조합 그리고 법률 부서가 사업 초기 단계부터 참여했기 때문에 성공할 수 있었다고 말했다. ■

통해중요한데이터에접속하는건수는1/4이상을 약간 상회하는 27%에 달했다. 앞으로 12-18개월 이내에 이 수치가 1/3 (35%)이상으로 증가할 것으로 조사응답자들은 전망했다. 또한, 다른 모바일 기기를 통해 중요한 데이터에 접속하는 경우도 현재의 1/5에서 30%로 증가할 것으로 예상되었다. 2011년 10월호 *이코노미스트지 (The Economist)* 는 새로운 소프트웨어와 관련 기기가 등장하게 됨에 따라, 앞으로 임원들이 회사 데이터에 접속함에 있어, 태블릿을 더 광범위하게 사용할 것이며, 언젠가 스마트폰도 대체하게 될 것으로 예상하였다. 넓어진 화면은 효과적으로 볼 수 있는 데이터의 범위를 확대하고, 외부 키보드 등의 보완을 통해 앱과의 손쉬운 상호작용을 가능케 한다.

흥미로운 점은, 응답자의 42%가 임원들이 가장 생산적이기 위해서는 전략기획 자료에 안전하고, 시의 적절하게 접속할 필요가 있다고 대답한 반면, 28%만이 모바일 기기를 통해 이러한 데이터에 접속하는 것이 적절하다고 답했다는 점이다. 당연히, 당면한 주요 도전과제는 잠재적인 보안과 기타 위험요인에 대한 우려이다. 그럼에도 불구하고, 본 설문조사에 참여한 응답자의 11%만이 사무실 밖에서 회사의 중요 데이터에 접속하는 것이 불가능하다고 응답했다. ■

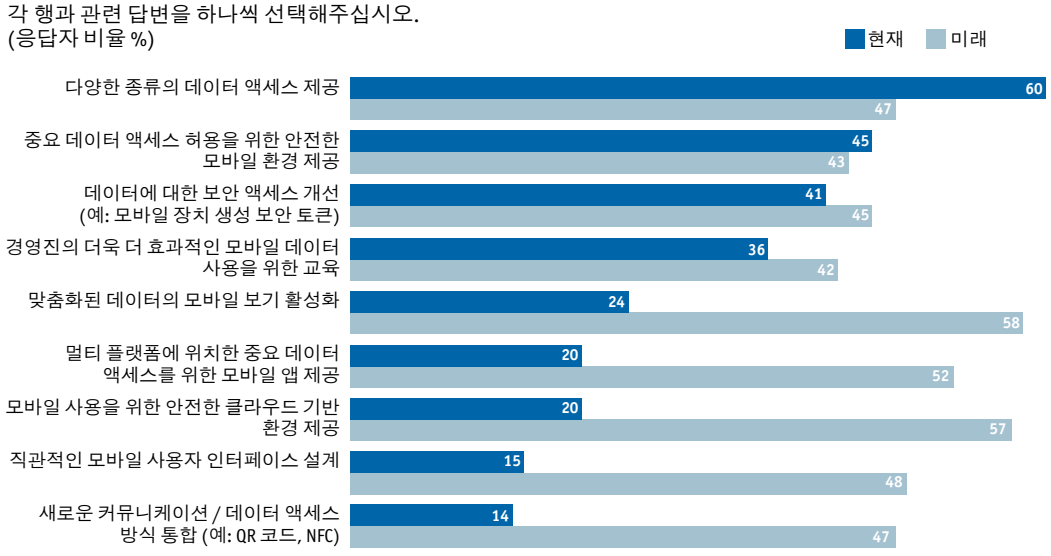
4 기업들이 효과적인 모바일 정책을 이행할 수 있는 방법은 무엇인가?

설문조사 응답자들은 모바일로 데이터를 접속하는 것의 이점과 이를 위해 필요한 투자에 대해 잘 인식하고 있다. 모바일 기기를 가지고 기업 데이터 에 안전하게 접속할 수 있도록 기업이 취할 수 있는 여러 조치 중 일부는 원격으로도 설치 가능하다. IT 관리자들은 지금도 기존의 관리 툴을 사용하여 노트북, 스마트폰, 태블릿에 보안 기능을 추가할 수 있다. 이들은 또한, 회사 및 개인 데이터를 구분할 수 있을 뿐 아니라, 회사 네트워크에 회사 데이터를 복사하고 저장할 수도 있다. 가상 데스크탑을 통해 개인 노트북에 저장되어 있는 데이터에 무선으로 안전하게 접속할 수 있다. 이러한 보호 조치는 적은 노력으로 분실 또는 파손된 기기에서의 데이터를 복구시키기도 한다. 본 연구소가 인터뷰한 임원들은 이러한 조치로 인해 앞으로 더 많은 임원들이 어떠한 컴퓨터에서도 안전하게 회사 데이터에 접속하게 될 것이라고 말했다.

출장 중인 임원들의 경우, 보안 프로토콜 업데이트에 적은 시간을 투자하게 됨에 따라 업무에 더 많은 시간을 쏟을 수 있게 된다. 앞으로, 데이터 그 자체를 보호하는 어플리케이션에 직접 탑재된 기술로 인해 데이터 보안은 더욱 강화될 것이며, 이는 데이터 가로채기나 악용을 더욱 힘들게 만들 것이라고

Q 모바일 권한 부여

귀사가 중요 데이터와 관련 액세스 권한을 부여하는 방법은 무엇이며 향후 어떻게 바뀔 것으로 예상하십니까? 각 행과 관련 답변을 하나씩 선택해주십시오.
(응답자 비율 %)



자료출처: 이코노미스트 정보수집 부서, 2012년 6월 (Economist Intelligence Unit survey, June 2012).

CSC의 티쿠(Tikoo)는 말했다.. "어플리케이션은 사용자가 업무를 수행함에 있어 아이패드를 사용하고 있는지 아니면, 작은 5인치 화면을 사용하고 있는지를 인지하고, 이에 맞게 데이터를 전송해야 한다"

레이몬드 (Raymond) 부사장은 그의 회사는 의무화하고 있지는 않으나, 공적 및 사적 용도의 환경을 분리하는 것이 중요하다고 말한다. 그러나, 이들을 둘러싼 정책이나 다른 보안정책들이 이행되지 않는다면, 이에 대한 대가를 치르게 될 것이라고 그는 말한다.책 동료들과의 대화 속에서 대기업의 보안이 얼마나 부풀려져 있는지를 항상 느끼게 되어 놀랍다고 그는 말한다. 필요한 정책들은 다 마련되어 있으나, 정책 이행이 이뤄지고 있지 않다는 것이다.

글로벌 리서치 기업인 입소스 (Ipsos)의 모든 직원은 회사 인트라넷을 통해 제공되는 보안관련 교육을 수료해야 한다. 이러한 방법은 84개국의 직원들을 교육시킬 수 있는 가장 비용 효과적인 방법이다. 미국 국가보안 연구소 (National Security Institute: NSI)와 같은 조직은 그들이 사용하는 프로그램을 내부적으로 개발하였지만, 지역적 필요에 따라 맞춤화할 수 있는 상업용 보안 교육 제품을 즉각적으로 제공하고 있다. 직원들은 또한 허용가능한 모바일 사용에 대한 정책에 서명해야 하는데, 이 정책은 이들이 모바일 기기를 통해 접속할 수 있는 데이터의 종류에서부터 암호 보안 수준에 대한 규칙에 이르기까지 관련된 모든 사항을 포괄하고 있다.

기타 보안상의 보호조치들은 사용자의 신뢰성 있는 행동을 통해서만 가능하다. 감사 및 기업준수 기업인 코얼파이어 (Coalfire)사는 비밀번호를 설정하고 있어야 하는 개인용 모바일 기기의 단 50%만이 비밀번호를 설정하고 있다고 말한다. BYOD 프로그램 하에서 직원들은 개인용 기기를 분실 또는 도난 당했을 때, 회사의 IT부서에서 회사 데이터를 보호하기 위해 해당 기기의 정보를 모두 삭제하는데 동의해야 한다.

기업 데이터에 대한 모바일 접속이 가능해짐에 따라 발생하는 보안상의 문제에 대해 직원들을 교육함에 있어 대부분의 기업이 개선의 여지가 있다. 설문조사는 유럽 및 북미 이외의 지역의 경영진은 개인용 기기에 대한 데이터 보안 정책을 거부할 가능성이 높음을 보여준다. 하지만, 점점 더 상호 연결된 비즈니스 환경에서, 한 지역에서의 보안 수준의 격차는 보안상 문제가 없는 다른 지역의 기업과 그들의 고객에게까지 영향을 미칠 수 있다. 보안 ■

5 결론

모바일 데이터 접속은 확대될 것이며, 이러한 움직임은 막을 수 없다. 이미 관리되지 않고, 안전하지 않은 기기가 비즈니스 환경에 침투되어, 회사 데이터를 위험에 빠트리고, 보안이 취약한 기기는 공격의 문을 열어주었다. 본 연구소의 설문조사 응답자의 약 1/3이 그들의 회사가 부적절한 수준의 모바일 기기 정책을 가지고 있다고 응답했다. 성공적인 모바일 데이터 접속 프로그램 달성을 위한 첫 단추는 합리적이면서도 실행 가능한 정책을 수립하는 것이다.

업계를 선두하는 모바일 기기 정책을 보유하고 있다고 응답한 임원들은 이동 중에 데이터를 사용함으로써 더 효과적이고, 협력적인 결정을 할 수 있게 되었고, 비즈니스 기회를 놓치는 경우가 줄어들었으며, 파트너와 고객과 효과적으로 일할 수 있게 되었다고 대답한다. 이러한 접속으로 인해 비즈니스 데이터가 손상되지 않기 위해 임원들은 리스크를 최소화하면서, 데이터 및 보안 서비스에 대한 투자를 지원하는 프로그램을 우선순위화 할 필요가 있다.

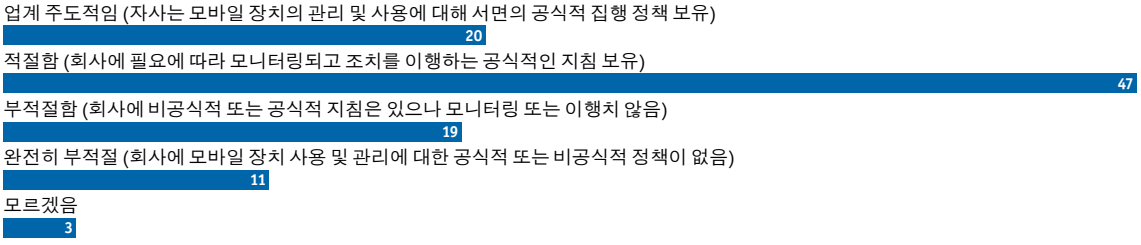
연결된 기기는 점점 더 글로벌 비즈니스 환경에서 중추적인 자리를 차지하고 있다. 사용하는 기기의 유형은 진화하고 있으며, 태블릿은 고객의 인기를 얻어가고 있다. 본 연구소는 차세대 소프트웨어 운영시스템이 출시되면, 앞으로 태블릿 사용은 폭발적으로 성장할 것이며, 태블렛은 스마트폰 보다 더 광범위한 데이터 접속 옵션을 제공하게 될 것이라 전망한다. 태블릿이 기존의 시스템을 대체하는 것이 아니라 보완하는 기기라는 점에서 애널리스트들은 이러한 현상이 장점과 단점 모두를 수반한다고 말한다.

앞으로, 중요한 데이터를 보호하기 위해서는 더 엄격한 액세스 요건을 갖춰야 할 지도 모른다. 일례로, 사무실 밖에서 업무용으로 태블렛을 사용하는 빈도가 늘어날수록, 임원들은 더 광범위한 데이터를 모바일로 접속할 수 있게 되며, 이는 새로운 도전과제를 불러일으킬 것이다. 그러므로, 기업들은 새로운 시각을 가지고 사용 가능한 인프라에서 사용할 수 있는 기기 및 이들 기기의 취약점에서부터 이용자에 이르기까지 모든 문제를 전면적으로 검토해야 할 것이다. ■

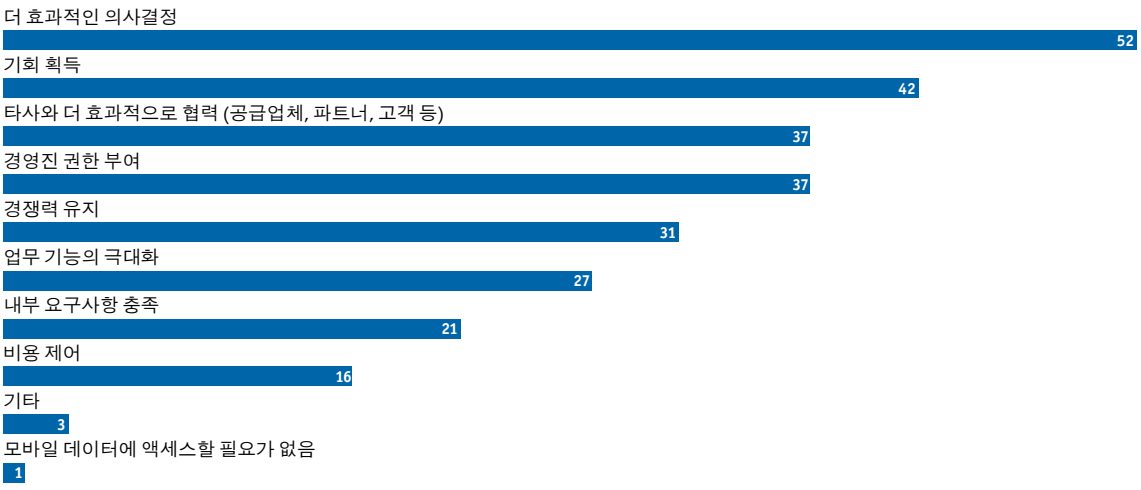
부록: 설문조사 결과

설문조사의 답변은 반올림 오차 또는 중복선택으로 인해 합계가 100%가 되지 않는다.

귀하의 조직의 모바일 장치 정책은 업계의 경쟁사와 비교할 때 어떠하다고 생각합니까?
(응답자 비율 %)

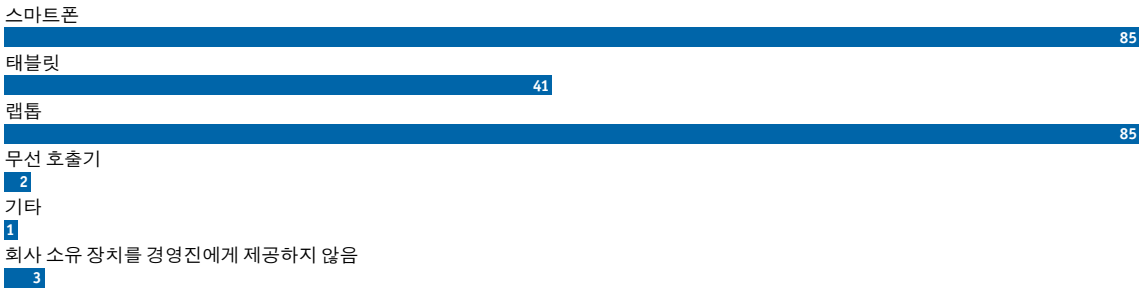


모바일 장치를 통해 중요 데이터에 액세스해야 하는 필요성을 주도하는 업무적 주요 요소는 무엇입니까?
3개까지 선택이 가능합니다.
(응답자 비율 %)



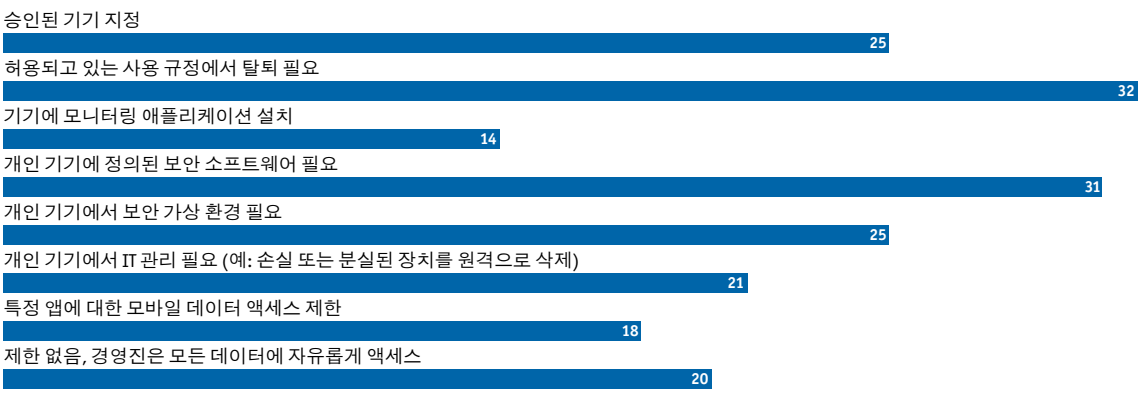
귀사에서는 사무실 외부에서의 중요 데이터 액세스를 허용합니까?
(응답자 비율 %)

귀사에서 임원에게 중요 데이터 액세스를 위해 제공하는 기기는 무엇입니까?
해당 항목을 모두 선택하십시오.
(응답자 비율 %)

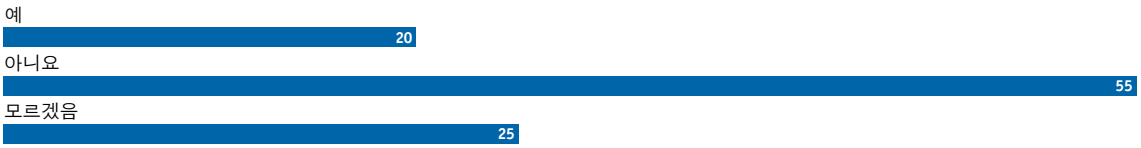


귀사에서는 회사 소유 기기를 대신한 개인 기기(BYOD)를 통한 중요 데이터 액세스를 허용합니까?
(응답자 비율 %)

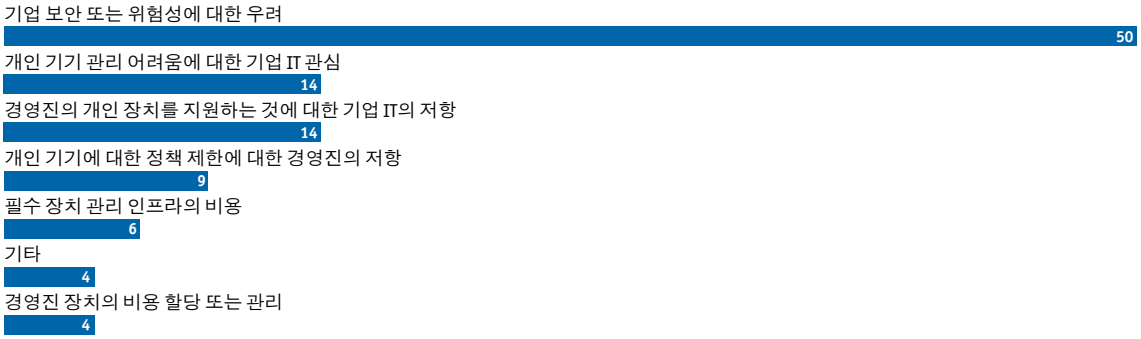
귀하의 회사에서는 중요한 데이터 액세스를 위해 BYOD를 어떻게 구현했습니까?
해당 항목을 모두 선택하십시오.
(응답자 비율 %)



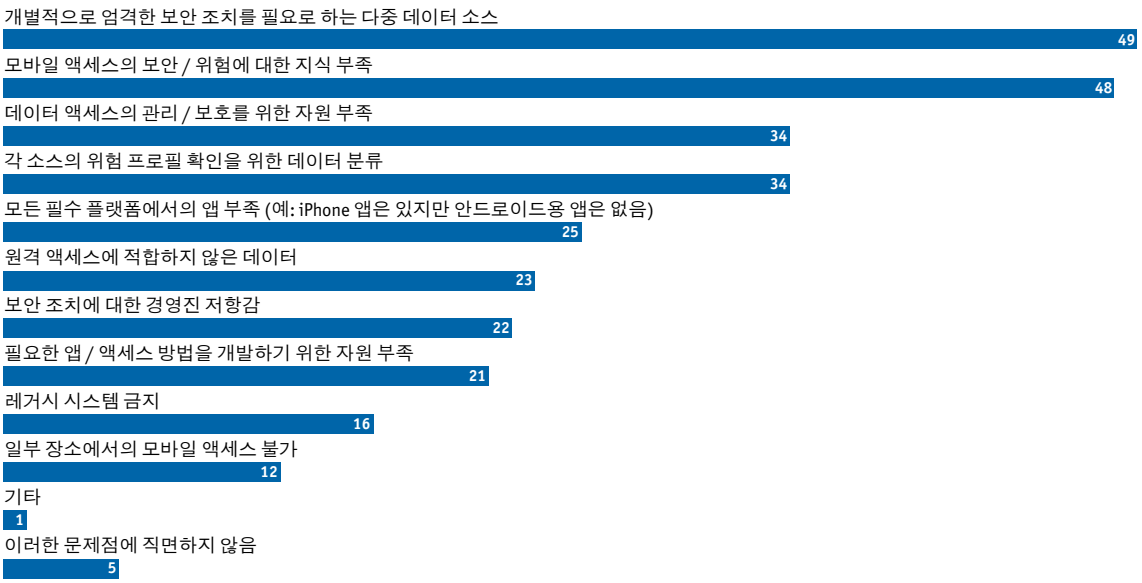
귀하의 조직에서는 중요 데이터 액세스를 위한 BYOD 를 구현할 계획이 있으십니까?
(응답자 비율 %)



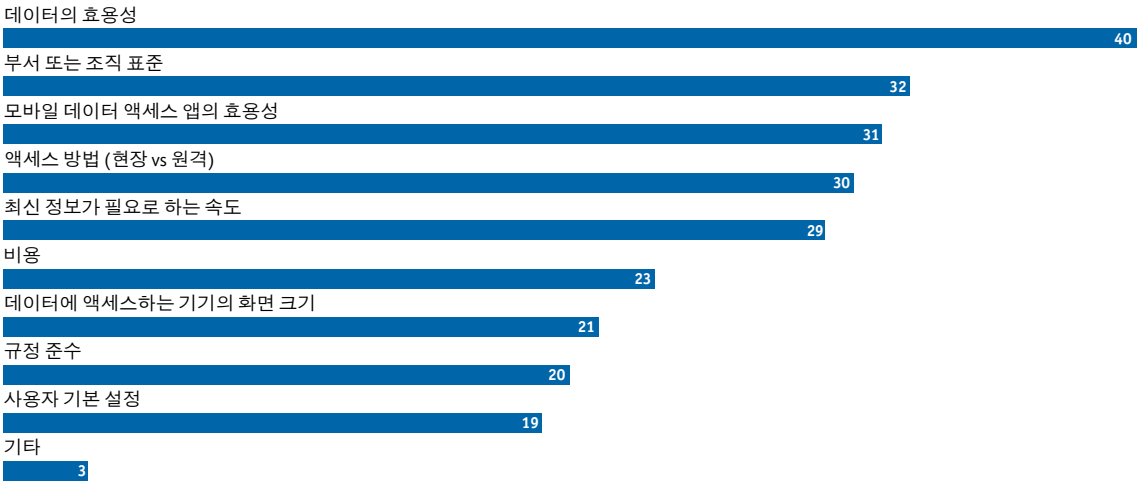
중요 데이터 액세스를 위한 BYOD 시현에 있어 가장 큰 장애물은 무엇이라고 생각하십니까?
(응답자 비율 %)



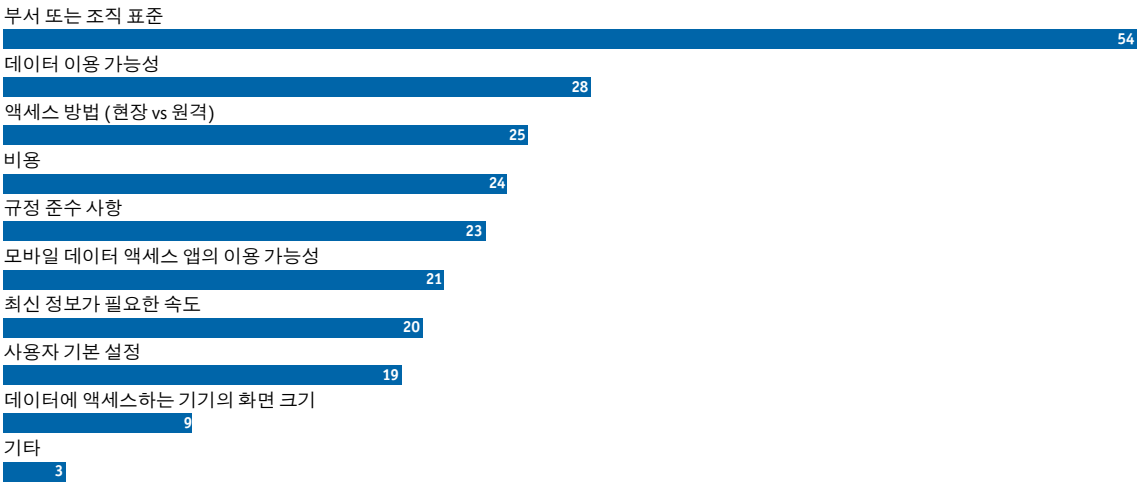
귀사가 회사 또는 경영진 소유의 휴대폰을 통해 중요 데이터를 액세스하려 할 때 직면하는 가장 중요한 문제점은 무엇입니까?
4개까지 선택이 가능합니다.
(응답자 비율 %)



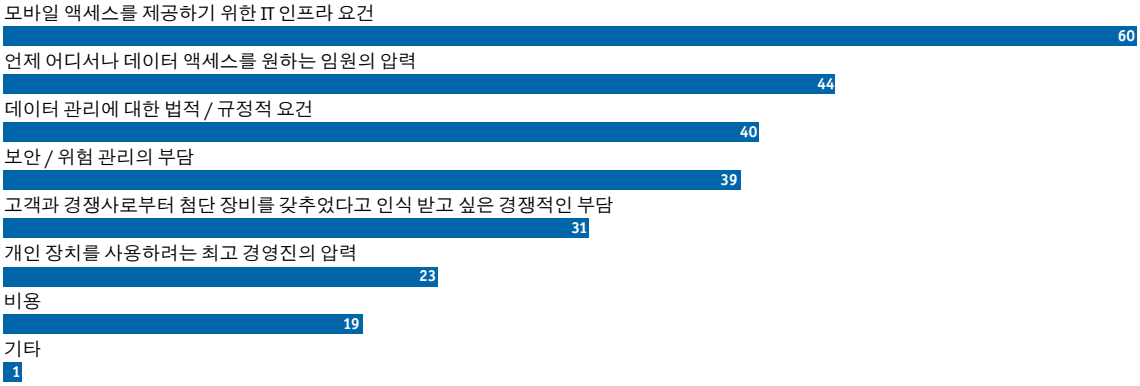
귀하의 직무 외 데이터의 모바일 기기 접속 여부를 결정하는 것은 무엇입니까?
3개까지 선택하십시오.
(응답자 비율 %)



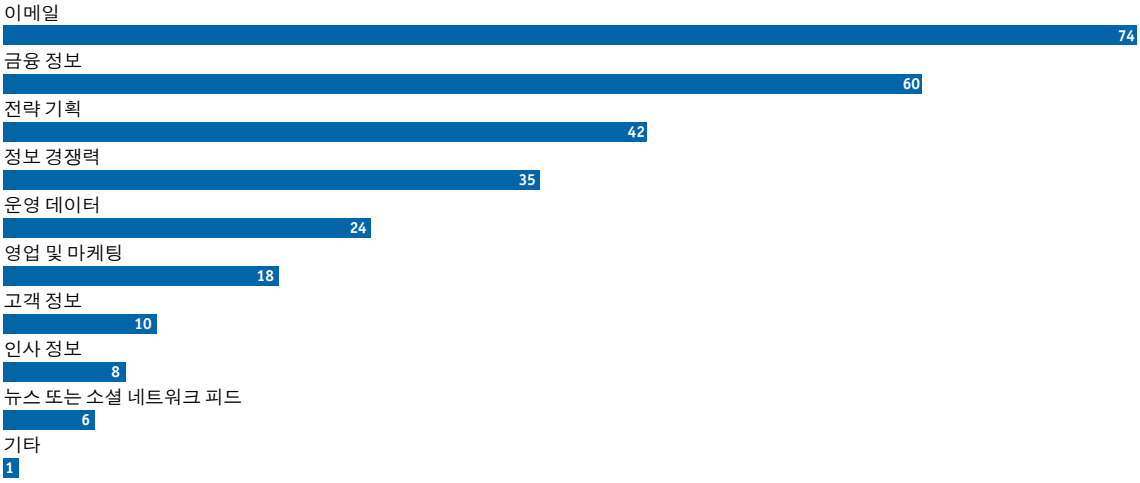
사용자의 모바일 기기를 통한 중요 데이터 액세스 승인 결정 기준은 무엇입니까?
3개까지 선택해 주십시오.
(응답자 비율 %)



모바일 장치 및 애플리케이션 전략을 구축과 관련 회사 정책과 접근방법에 가장 중요한 영향을 끼치는 것은 무엇입니까?
3개까지 선택하실 수 있습니다.
(응답자 비율 %)

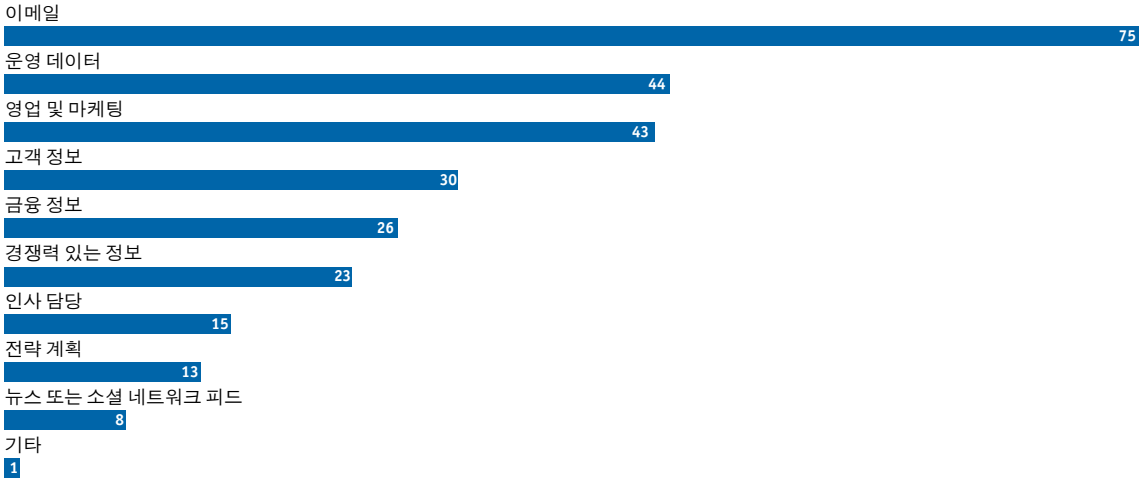


다음에 표시된 직책의 생산적인 업무 수행을 위해 안전하게, 또한 시기적절히 제공되어야 하는 정보는 나열된 목록 중 어느 것입니까? — 임원
각 역할 별 3 개까지 선택이 가능합니다.
(응답자 비율 %)



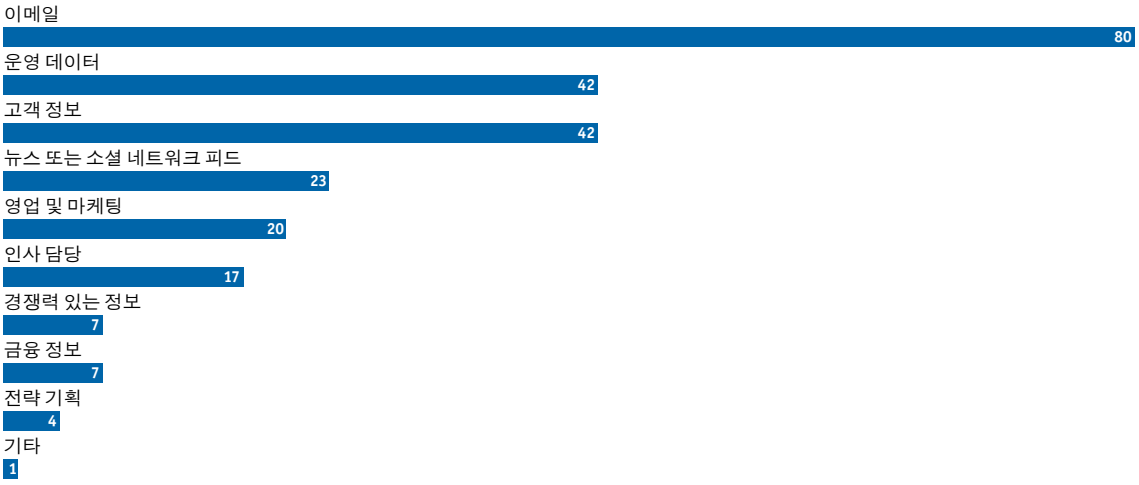
다음의 역할을 가장 생산적으로 수행하기 위해 안전하고 시기 적절하게 제공되어야 하는 정보는 다음 중 어느 것입니까? — 비즈니스 관리자

각 역할에 따라 3 개까지 선택 가능합니다.
(응답자 비율 %)



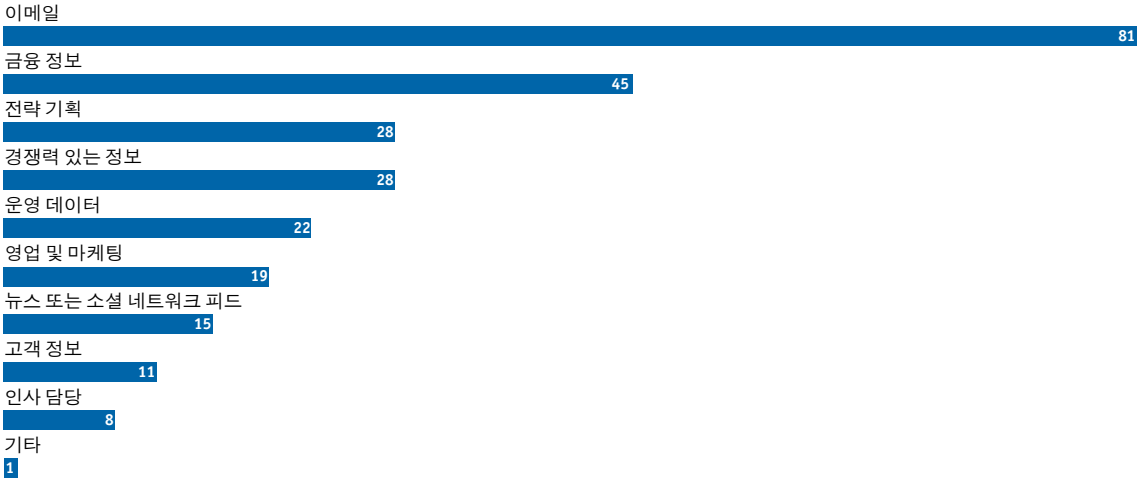
다음의 역할의 가장 생산적인 수행을 위해 안전하고 시기 적절하게 제공되어야 하는 정보는 다음 중 어느 것입니까? — 직원

각 역할에 따라 3 개까지 선택 가능합니다.
(응답자 비율 %)



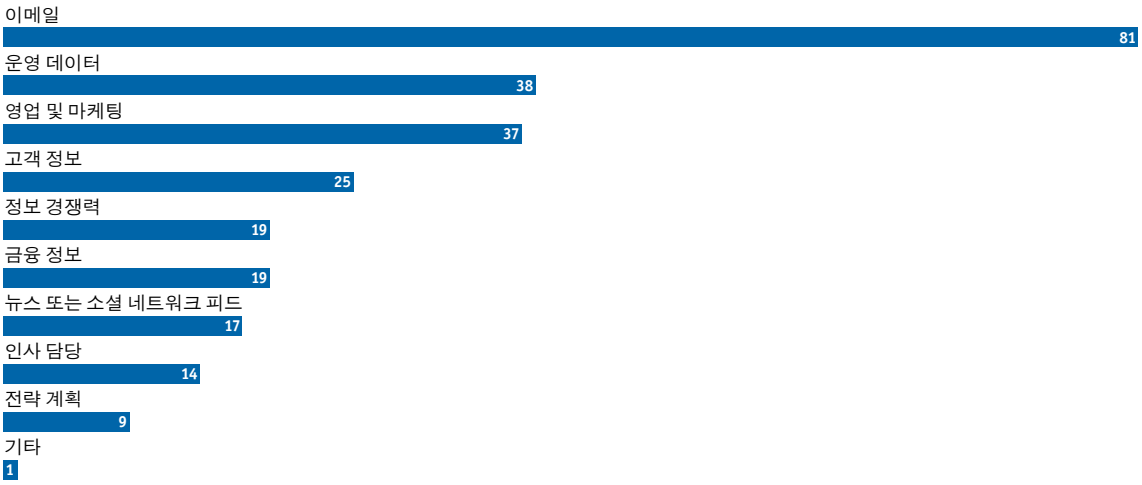
다음 중 모바일 장치에서 액세스하기에 적합한 정보 / 미디어의 종류는 어느 것입니까?
— 임원

각 역할에 따라 3 개까지의 선택이 가능합니다.
(응답자 비율 %)



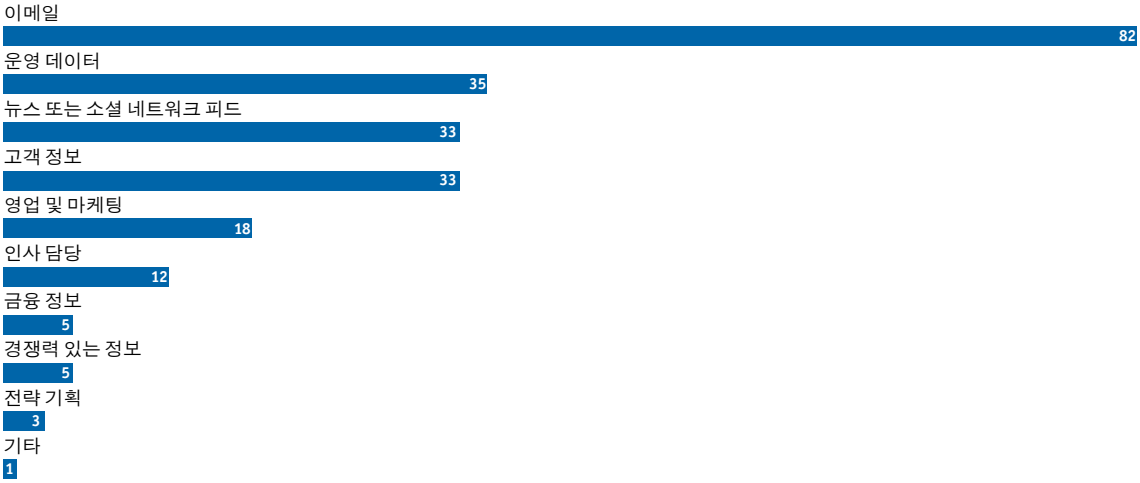
다음 중 모바일 장치에서 액세스하기에 적합한 정보 / 미디어의 종류는 어느 것입니까?
— 비즈니스 관리자

각 역할에 따라 3 개까지 선택 가능합니다.
(응답자 비율 %)



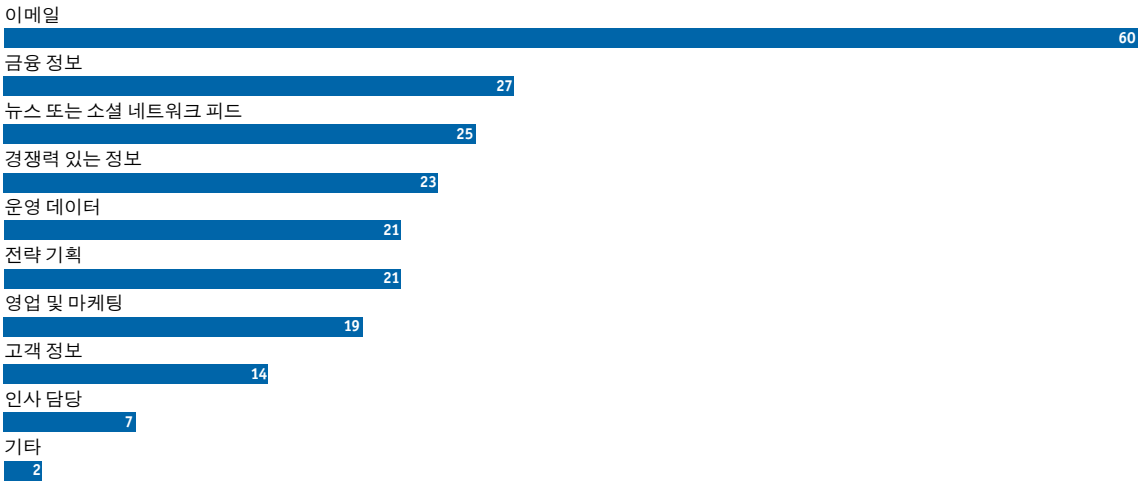
다음 중 모바일 장치에서 액세스하기에 적합한 정보 / 미디어의 종류는 어느 것입니까? — 직원

역할에 따라 3 개까지 선택이 가능합니다.
(응답자 비율 %)



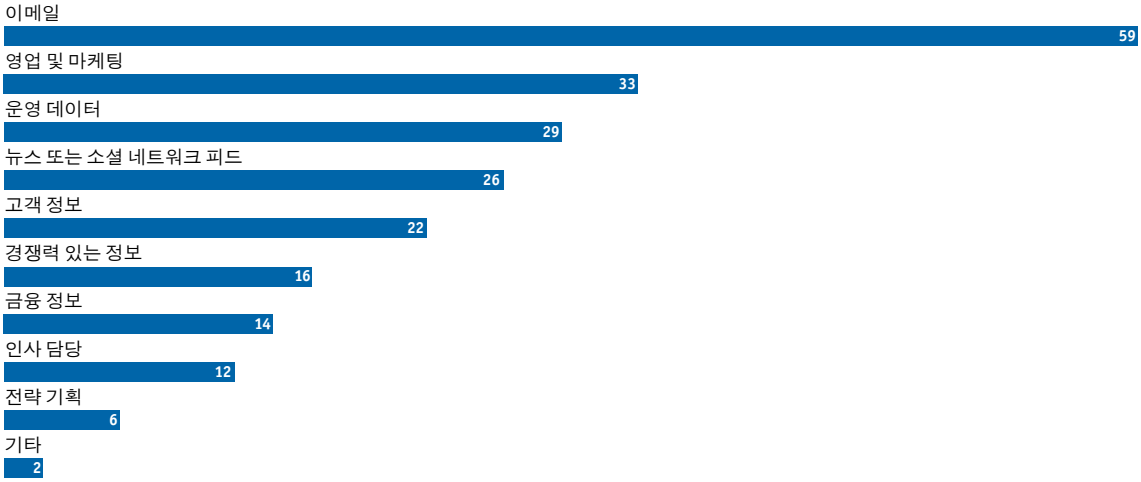
다음 중 클라우드 기반 스토리지에서 모바일 장치를 통해 액세스하기에 적합한 정보 / 미디어의 종류는 어느 것입니까? — 임원

각 역할에 따라 3 개까지 선택 가능합니다.
(응답자 비율 %)



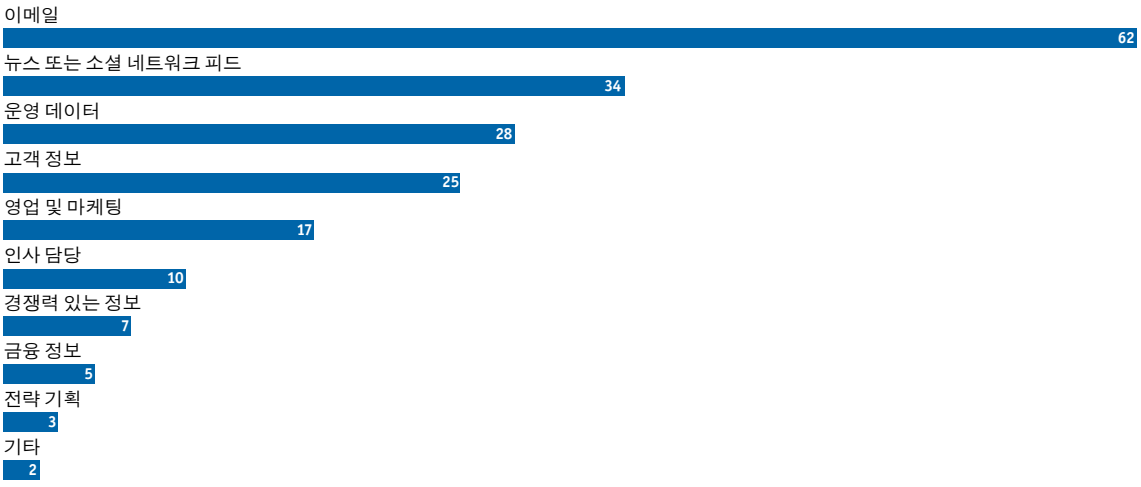
다음 중 클라우드 기반 스토리지에서 모바일 장치를 통해 액세스하기 적합한 정보 / 미디어의 종류는 어느 것입니까? — 비즈니스 관리자

각 역할에 따라 3 개까지 선택 가능합니다.
(응답자 비율 %)



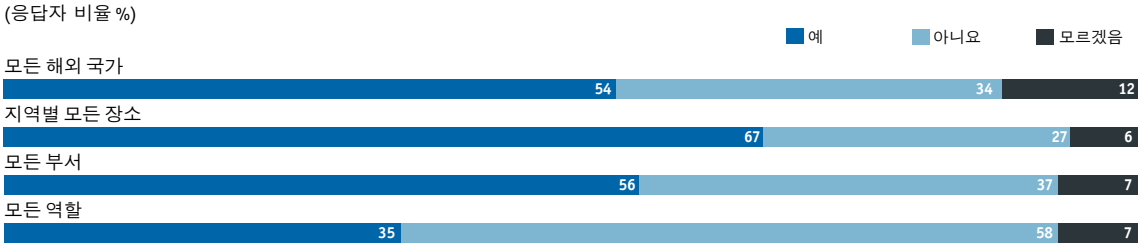
다음 중 클라우드 기반 스토리지에서 모바일 기기를 통해 액세스하기 적합한 정보/미디어의 종류는 어느 것입니까? — 직원

각 역할에 따라 3개까지 선택 가능합니다.
(응답자 비율 %)



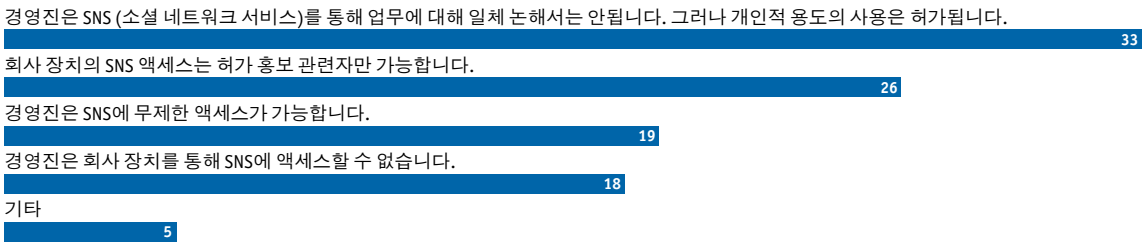
귀하의 회사에서는 다음의 각 그룹의 데이터에 모바일 액세스를 제공합니까?

(응답자 비율 %)

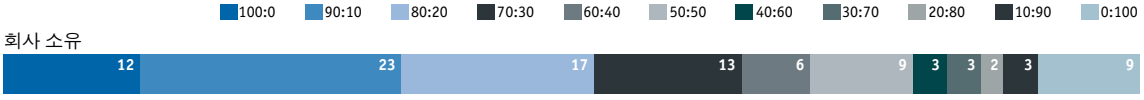


귀하의 조직에서는 회사 기기를 통한 소셜 네트워크 (예: 페이스북, 트위터) 사용을 허락하는 정책을 보유하고 있습니까?
(응답자 비율 %)

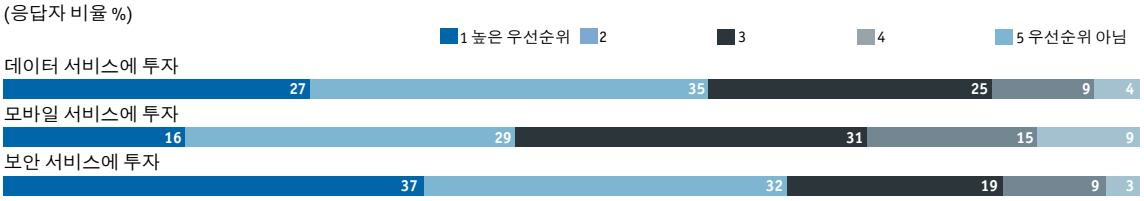
귀사는 회사 장치를 통한 소셜 네트워크 사용과 관련 어떤 규정을 보유하고 계십니까?
(응답자 비율 %)



귀사에서의 모바일 기기 이용시간을 비교했을 때 회사 소유 기기와 개인 소유기기의 이용 비율은 어떻게 됩니까?
슬라이더 버튼을 이용해 옵션 비율이 가장 잘 반영된 관련 비율을 선택하십시오 (예: 60% - 40%).
(응답자 비율 %)

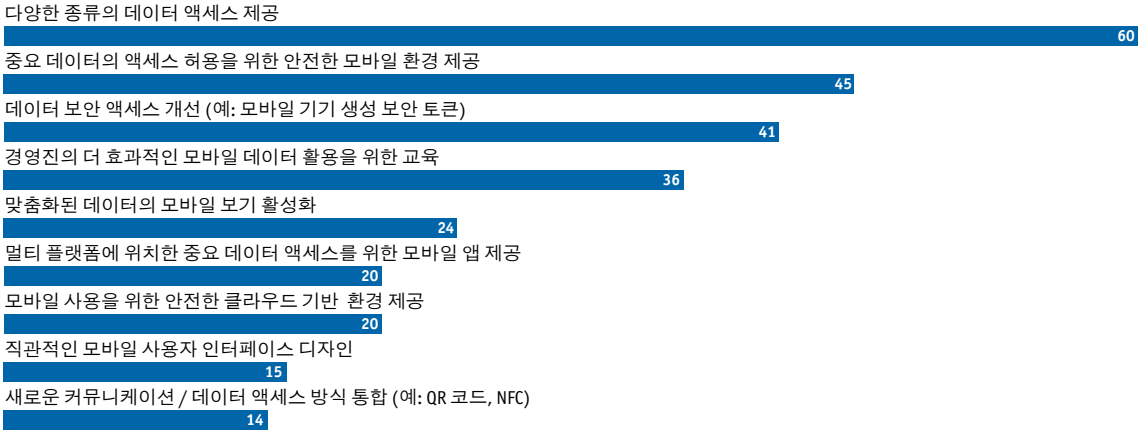


다음 전략과 관련 귀하의 조직의 우선순위는 무엇입니까?
평가등급은 1에서부터 5까지이며, 1은 높은 우선순위를, 5는 우선순위 아님을 나타냅니다.
(응답자 비율 %)



귀하의 회사가 중요 데이터와 관련 액세스 권한을 부여하는 방법은 무엇이며 향후 어떻게 바뀔 것으로 예상하십니까? —현재

각 행과 관련 열에서 하나의 답변을 선택하십시오.
(응답자 비율 %)



귀하의 회사가 중요 데이터와 관련 액세스 권한을 부여하는 방법은 무엇이며 향후 어떻게 바뀔 것으로 예상하십니까? —미래

각 행과 관련 열에서 답변 하나를 선택하십시오.
(응답자 비율 %)

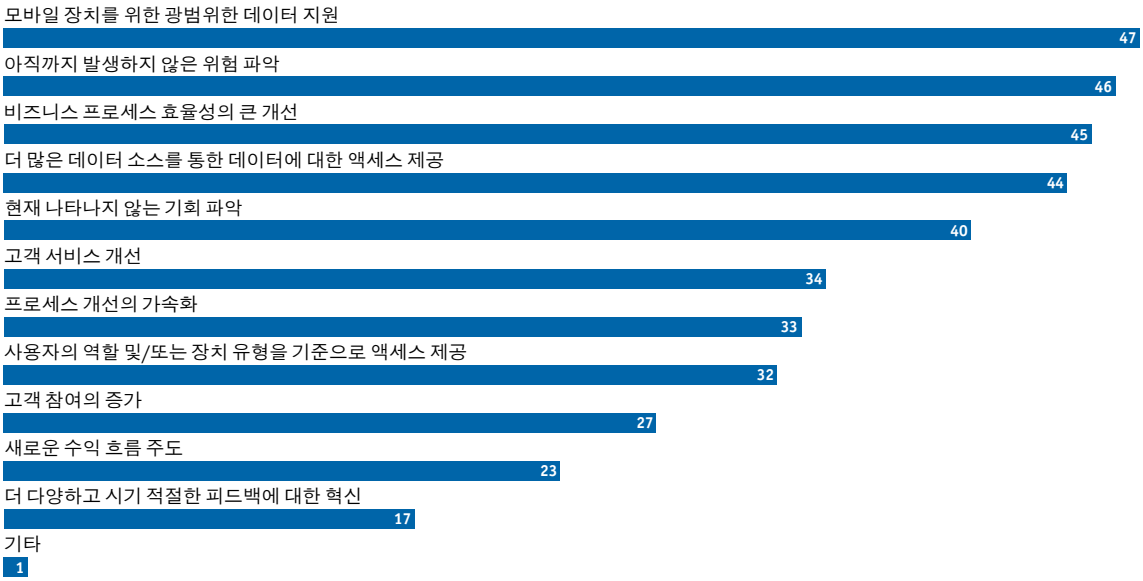
현재 중요한 데이터를 모바일 채널을 통해 접속하는 정도는 얼마나 됩니까?
답변 합계는 100%가 되어야 한다.

	평균
스마트폰을 통한 모바일 접속	26.9
다른 기기를 통한 모바일 접속 (예: 태블릿)	21.7
모바일 접속하지 않음	59.8

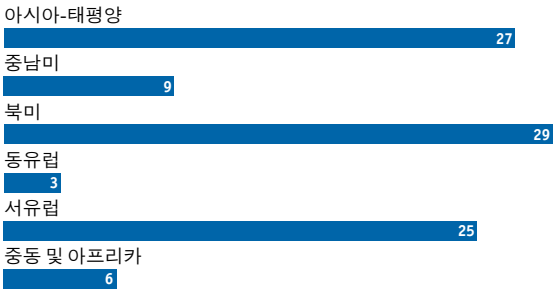
12-18개월 이내에 중요한 데이터를 모바일 채널을 통해 접속하는 비중은 얼마나 될 것으로 예상합니까?
답변 합계는 100%가 되어야 합니다.

	평균
스마트폰을 통한 모바일 접속	34.5
다른 기기를 통한 모바일 접속 (예: 태블릿)	30.2
모바일 접속을 하지 않음	42.8

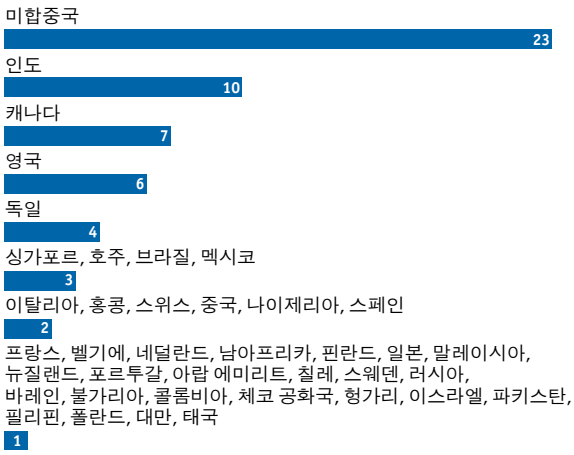
향후 12 - 18개월 동안 현재는 액서스가 불가능한 중요 데이터와 관련 실행하고자 하는 것은 무엇입니까?
해당 항목을 모두 선택해 주십시오.
(응답자 비율 %)



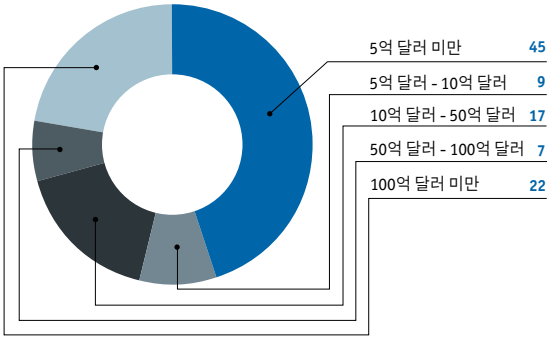
귀하가 현재 위치한 곳은 어디입니까?
(응답자 비율 %)



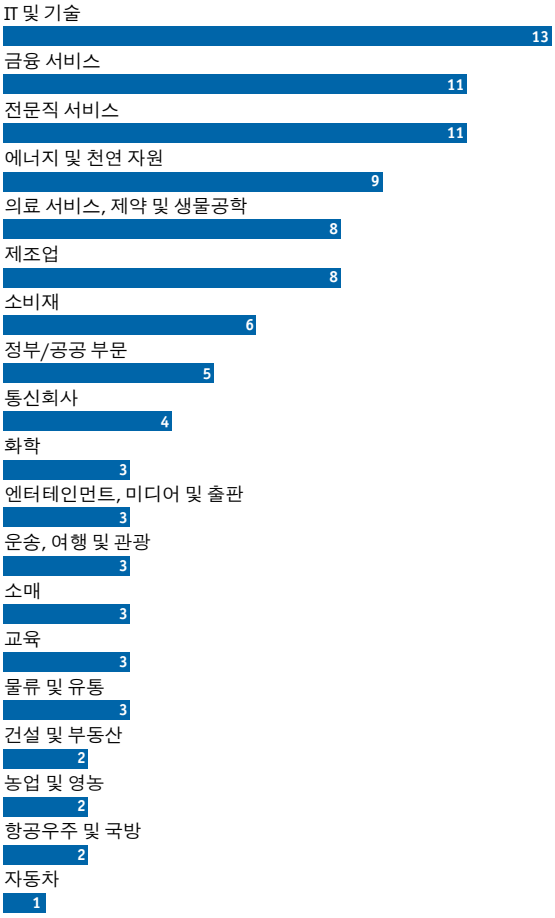
귀하가 현재 위치한 곳은 어디입니까?
(응답자 비율 %)



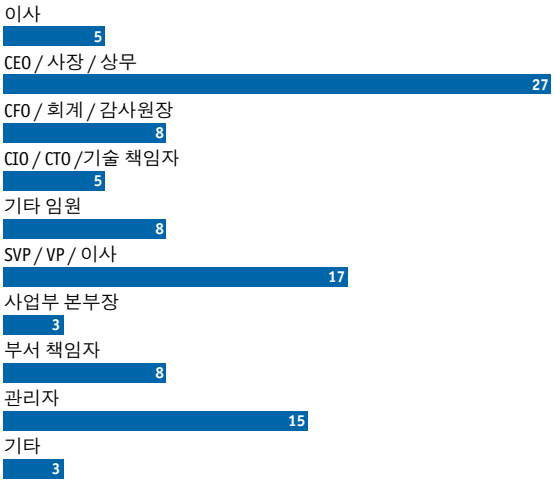
귀사의 전세계 매출은 미국 달러 (USD)로 얼마입니까?
(응답자 비율 %)



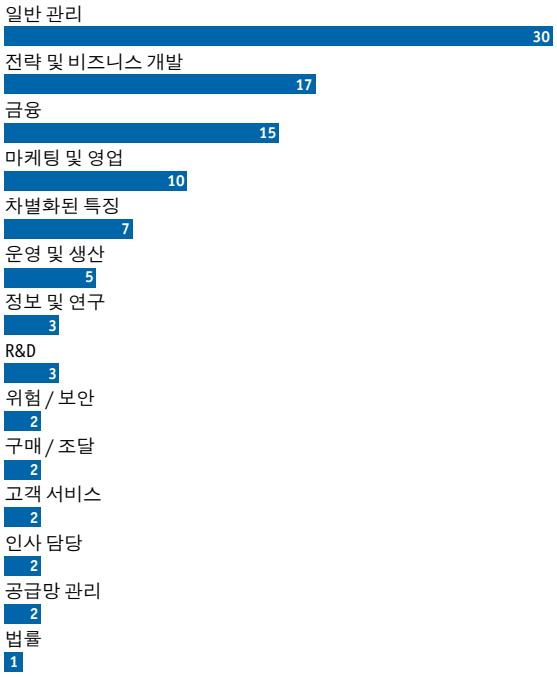
귀하의 주요 업종은 무엇입니까?
(응답자 비율 %)



다음 중 귀하의 직함을 가장 잘 설명하는 것은 어느 것입니까?
(응답자 비율 %)



귀하의 직무는 무엇입니까?
(응답자 비율 %)



표지 일러스트: Shutterstock

런던
26 Red Lion Square
London
WC1R 4HQ
England
전화: (44.20) 7576 8000
팩스: (44.20) 7576 8476
이메일: london@eiu.com

뉴욕
750 Third Avenue
5th Floor
New York, NY 10017
United States
전화: (1.212) 554 0600
팩스: (1.212) 586 0248
이메일: newyork@eiu.com

홍콩
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
전화: (852) 2585 3888
팩스: (852) 2802 7638
이메일: hongkong@eiu.com

제네바
Boulevard des
Tranchées 16
1206 Geneva
Switzerland
전화: (41) 22 566 2470
팩스: (41) 22 346 93 47
이메일: geneva@eiu.com