보안 모니터링부터 사이버리스크 모니터링까지

비즈니스와 조율된 사이버 보안의 실현

저자 Adnan Amjad, Mark Nicholson, Christopher Stevenson, Andrew Douglas
일러스트레이션 Lucy Rose

왜 *우리는* 리스크를 탐지하지 못했나?

이는 대규모 사이버 보안 사고가 발견되거나 발표될 때 마다 항상 나오는 질문이다. 데이터 침해 사건의 70% 가량이 조직의 자체 보안 운영팀이 아닌 제3자에 의해 탐지되며,[1] 이는 현재 대부분의 보안 모니터링 방법론이 적절치 않음을 방증한다.

비즈니스의 관점에서 보자면, 최신 탐지 기술에 기업이 쓴 모든 돈을 고려할 때[2] IT부서는 모든 것을 탐지할 수 있어야 한다. 그렇지 않은가? 아이러니하게도, 그렇게나 많은 사이버 침입이 발각되지 않는 이유는 아마 IT부서가 너무나 많은 것을 잡아내고 있기 때문일 것이다. '눈을 화면에 고정한' 사람들이 매일 수십 개 또는 수십 만 개의 경고를 보면서 판단하고 있다.[3] 적절한 기술을 가진 인재의 부족은 문제를 더 악화시킨다.[4] 더 심각한 것은 이런 경보가 끊임없이 발생한다는 것이다. 시스코(Cisco)의 추정에 따르면 인터넷 트래픽은 2014년에서 2019년 사이에 연평균 23%의 성장률을 보일 것이라고 한다.[5]

데이터와 데이터 공유, 그리고 이 모든 것을 움직이는 미로 같은 연결성이 보안 문제의 핵심이다. 환경이 갈수록 복잡해지면서, 범죄자들이 악용할 수 있는 취약점도 기하급수적으로 늘어나며, 탐지를 피할 수 있는 방법도 많아지고 있다.[6] 정보보안팀은 수백만 개의 기기, 탐지 기술, 기타 출처에서 쏟아져 들어오는 IT 데이터로 정신을 차리지 못할 지경이다. 무엇이 중요한지를 탐지하는 것이 빅데이터 관련 문제 중에서도 가장 심각한 문제다. 여전히 많은 조직이 적절한 데이터에 접근하지 못하고 있거나 적절한 데이터의 가용 여부를 알기 위해 다른 부서들과 협력하지 않는 것 또한 문제다.

하지만 이는 일각에서 시사하듯 '건초더미에서 바늘 찾기' 같은 문제는 아니다. 그렇다. 위협 탐지는 모든 데이터를 걸러낼 수 있는 더 나은 자동화된 정보 시스템이 필요하다. 하지만 최신 기술만으로는 이 문제를 해결할 수 없다. IT 보안 감시는 사이버리스크 모니터링이 되어야 한다. 기업은 단순한 악의적인 사이버 활동의 감시보다는 비즈니스에 가장 큰 손실을 끼치는 활동들을 사전에 포착하고, 리스크 경감을 위한 의사결정을 지원할 수 있는 기능이 필요하다.

당연히 이런 기능은 조직마다 다른 형태로 나타나겠지만, 새로운 접근법은 다음의 두 가지 기본 요소를 반드시 포함해야 한다.

- **비즈니스적 맥락.** 아이러니하게도 모든 IT 데이터의 의미를 밝히려면 넓은 비즈니스 영역에 대한 더 많은 데이터가 필요하다. 하지만 단순한 데이터 수집보다 중요하고 훨씬 어려운 일은, 비즈니스적 맥락에 맞는 IT 데이터 간의 연관성을 찾는 일이다.

- **비즈니스 리스크에 관한 지침.** 사이버 위협이 어떻게 비즈니스에 주로 영향을 미칠 수 있는지에 대해 기술팀은 명확히 알고 있어야 한다. 이를 위해서는 모든 사업부서와 기술팀의 참여가 필요하며, 이후 중요한 사항을 파악하기 위한 모니터링의 방식을 정할 수 있다.

진정으로 리스크에 초점을 맞춘 모니터링 기능이 있다면, 조직은 비즈니스 전략을 좀 더 자유롭고 안전하게 추진할 수 있다. 그러나 이런 전환은 기술 담당 리더나 기술 팀의 노력으로만 이뤄지지 않는다. 이는 경영진의 지도, 협력, 지속적인 거버넌스가 필요하다.

모니터링 실패

심지어 많은 선진적인 기업들조차 보안 모니터링에 있어 기술 주도적 접근법을 취한다. 이러한 접근법의 위험성을 가상의 차량 렌탈 기업인[7] 드라이브나이스(DriveNice)의 사례를 통해 알아보자. 누군가 이 회사를 목표로 멀웨어 공격을 감행했다. 매우 간략화된 설명이지만, 이 가상 시나리오는 조직들이 직면한 매우 일상적이고 현실적인 위험을 반영한다(다음 페이지 참조).

드라이브나이스의 정보보안팀은 상대적으로 인원이 적은 편이긴 하나 딱히 약점이 있다고 생각할 만한 이유가 없었다. 정보보안 최고 책임자(CISO)는 수십 개의 스크린을 모니터링하는 그녀의 팀이 선진적 관행을 잘 따르고 있으며, 다양한 보안 툴에서 공급받는 수많은 데이터를 집중화하고 상관관계를 파악할 수 있게 해주는 기술 투자 이후에는 더욱 개선되었다고 믿는다. 정보보안팀은 최근 운영센터를 업그레이드했고, 데이터 손실 방지 추진계획에도 착수했다. 또한 잠재적인 악의적 공격의 트렌드를 이해하기 위해 사이버 위협 관련 정보를 구입한다. 회사의 인프라가 매우 광범위하고 다양하지만, 정보보안팀은 중요 시스템들에 대한 패치 작업을 매우 잘 수행한다. 비록 중앙 관제팀이 확보한 네트워크 전체에 대한 가시성은 부족했지만, CISO는 적극적으로 소통하도록 그들을 장려하고, 또한 정기적으로 컴플라이언스 시험을 실시한다.

드라이브나이스에 벌어진 일은 나이스하지 않았다.

드라이브나이스는 다섯 대륙의 지역 기업들로 구성된 세계적인 차량 렌탈 브랜드로, 직영 및 프랜차이즈 지점이 하나의 브랜드로 운영되고 있다. 각 지역과 지점은 약간씩의 차이만 있는 유사한 기술 플랫폼을 운용하고, 지역별 그리고 중앙 집중적인 IT 및 보안 운영체제를 혼용해 사용한다. 여러 서비스 제공자를 통해 제공되는 클라우드 기반 시스템을 이용하는데, 이는 드라이브나이스가 지리적 확장에 맞춰 빠르게 시스템을 확장할 수 있게 해준다.

독일에 위치한 프랜차이즈 지점의 어느 프론트 데스크 직원이 드라이브나이스 이메일 주소를 가진 이메일을 열어 별다른 이상이 없어 보이는 첨부문서를 클릭한다. 하지만 이 메시지는 비활성화되지 않은 이전 계약업자의 이메일 계정에서 온 것이었다. 이메일에 첨부된 파일은 실은 멀웨어로, 회사 시스템 전체에 빠르게 퍼져나갔다. 몇 주 후, 중앙 관제팀의 하급 분석가가 이 멀웨어를 발견해 낮은 위험도를 가진 일상적 위협으로 분류한다. 이는 회사의 침입 탐지 시스템에서 자동으로 생성된 경고에 따른 결정이다.

IT부서는 이런 사건을 지역 수준에서 관리하므로, 분석가는 이 사건에 대한 짧은 보고서를 작성해 지역 본부로 보내고 후속조치를 기다린다. 불행히도, 분석가는 경고를 생성하는 실제 시스템에 직접 접근이 불가능하므로, 이 보고서는 제한적인 정보만을 담아 발송된다. '낮은 위험 수준' 으로 분류된 탓에, 분석가는 이 사건을 지역 본부로 보고한 후 종료된 것으로 생각한다. 그 후 시스템 조율을 위한 잘못된 시도로, 분석가는 같은 유형의 사건이 추후 발생하면 무시하도록 탐지 시스템의 설정을 바꾼다.

몇 주 후, 3백만 명의 고객 결제 기록이 사이버 범죄자 웹게시판에 매물로 나타난다. 드라이브나이스는 기자가 홍보 부서에 전화를 걸어 질문을 하자 그제서야 사태를 알게 된다.

IT 부서에서 보안 침해의 원인을 파악하고 여러 보안팀들의 협조를 구하느라 허둥대는 사이, 이미 멀웨어는 2단계 활동을 시작한다. 멀웨어는 평범한 낮은 수준의 위협이 아니었던 것으로 드러난다. 해커가 드라이브나이스를 목표로 멀웨어를 맞춤 제작하여, 고객 포인트 시스템인 나이스리워즈(NiceRewards)에 접근할 수 있는 코드를 심고, 고객 계정의 포인트 잔액을 조작한 것이다. 나이스리워즈 플랫폼이 클라우드 기반이기 때문에 드라이브나이스의 통제와 가시성은 매우 제한적이다. 엔지니어들은 이 포인트 시스템에서 발생한 보안 사고를 회사의 보안 모니터링 시스템에 통합해 관리할 수 있는 능력을 가지고 있지 않았다.

회원들이 포인트 잔액이 부정확하다는 항의를 시작하자, 나이스리워즈 팀은 비즈니스 로직에 문제가 있을 가능성을 조사하기 시작한다. 이와는 별개로, 사기 대응팀에서 의심스러운 고객 포인트 사용 동향을 포착한다. 평소보다 많은 고객들이 포인트를 상품권 또는 파트너사의 포인트로 바꾸고 있다. 사기 대응팀과 스피디리워드(SpeediReward)팀은 비즈니스 분석과 앞서 발생한 해킹 사건에 매우 깊이 몰두하느라 바쁜 나머지 새로운 문제를 제대로 신경 쓸 여력이 없다.

한 달이 지나고 나서야 누군가가 이 세가지 사건을 연결 짓게 된다. 즉 결제 기록의 도난, 나이스리워즈 잔여 포인트 불일치, 부정한 현금화 등이 동일한 멀웨어 사고와 연관이 있다는 것을 알게 된 것이다. 이 때쯤에는, 고객 불만도 점점 커져서 결제기록 도난으로 발생한 비용이 엄청나게 발생하게 되며, 드라이브나이스는 부정적인 언론보도로 매출에 타격을 입을까 두려워하게 된다. 잠재적 손실을 막기 위해 보상 프로그램 사업 파트너들이 드라이브나이스와의 협업을 중단하고, 프랜차이즈 가맹점들의 불만도 심화되고 있다. 본사가 지금쯤이면 문제를 해결했어야 하는 것 아닌가?

무엇이 잘못된 것인가?

드라이브나이스의 보안 침해 사고를 개인의 잘못이나 실수 탓으로 돌리기 쉽다. 하지만 회사의 보안 모니터링에 대한 IT 중심의 접근법이 해킹 탐지 실패와 공격의 전체 규모 파악에 몇 주가 걸린 원인이다.

첫째, 드라이브나이스는 멀웨어가 처음 메일 서버에 나타났을 때 초기 경고 신호를 놓쳤다. 흔히 그렇듯이 사이버 위협 정보 시스템이 아직 멀웨어의 소스를 악성으로 분류하지 않은 탓에 처음 다운로드 발생 시 멀웨어는 해킹 탐지를 피할 수 있었다. 멀웨어가 흔히 알려진 유형과는 많이 달라 보안 툴이 미처 탐지할 수 없었던 것이다.[8] 하지만 다른 신호가 없었던 것은 아니다. 프론트 데스크의 해당 직원이 예상하기는 어려웠겠지만, 멀웨어 링크를 포함한 피싱 이메일 주소는 과거 계약 업체의 이메일 주소였고, 이 계정은 이미 몇 달 전에 비활성화 되어야 했다. 만약 정보보안팀이 수많은 IT 시스템 데이터에 더해 인사 부서에서 받은 최신정보를 활용했다면, 오래된 계정의 사용을 탐지하고 즉시 경고를 발령했을 것이다.

둘째, 보안 팀이 멀웨어를 탐지했을 때도 이 공격이 매우 심각하며, 회사를 목표로 했다는 점을 파악하는 데 실패했다. 분석가의 조치는 그에게 배정된 많은 관제 대상 스크린의 수와 탐지 시스템이 제공하는 제한된 정보로 인해 영향을 받았다. 게다가 어떤 지역에서 동일한 유형의 사건이 발생하는지 보여주지 못하는 시스템의 한계로 인해 분석가의 행동은 제약을 받았다.

책임을 전가하는 문화 또한 문제를 키웠다. 여러 팀들이 관여하게 되면 문제를 '붙잡으려'하기 보다는 '떠 넘기기'가 쉽다. 많은 기업들이 그렇듯 드라이브나이스는 일관된 감독과 중앙집중적 업무흐름 관리가 이뤄지지 않았다. 이런 요인들과 인적 과실이 결합되어 앞으로 유사한 사건이 발생하면 이를 시스템이 무시하도록 설정이 바뀌게 되었다. 이는 적절한 지식이나 훈련이 부족한 하급 직원이 의사결정을 내리도록 방치될 때 흔히 발생하는 일이다.

마지막으로, 분석가가 멀웨어의 심각성을 깨달았을 때, 해커의 두 번째이자 보다 근본적인 공격 동기를 파악하지 못했다. 신용카드 정보가 해킹되었다는 사실을 알게된 후, 대응팀은 제한적인 분석과 대응 과정에만 집중했고 업무 과다로 인해 다른 공격에는 관심을 두지 못했다. IT 부서 자체의 조직화도 엉망이었고, 중앙 보안 관제팀은 관련된 지역 시스템을 거의 들여다보지 못했다. 통합되지 않은 제3자 제공 클라우드 서비스를 이용하는 바람에 상당한 규모의 보안 사각지대가 생겼다.

설상가상으로 현업에서도 의사소통이 제대로 이뤄지지 않았는데, 이는 많은 임원들이 익숙해지게 될 장애물이다. 나이스리워즈 부서는 고객들이 계정 관련 문제로 불평하고 있다는 것을 알았고, 사기 대응팀도 포인트 관련 의심스러운 활동을 추적하고 있었지만, 아무도 IT부서의 협조를 구하지 않았다. 그랬다. 이 정보를 연관 짓는 것은 수작업에 가까운 일이었겠지만, 사이버 관제팀, 사기 대응팀, 고객 보상 팀이 함께 고민했다면 이 해킹의 전모가 훨씬 더 빨리 드러났을 것이다. 게다가 CISO가 동종업계 또는 사법기관과 정보를 공유했다면, 경쟁사도 유사한 공격을 경험했다는 것을 알게 되어 멀웨어의 기능에 대해 훨씬 깊은 통찰을 얻었을 것이다.

드라이브나이스의 보안 모니터링에 대한 접근법은 IT중심적이었다. 그 결과 이 회사는 기술적, 조직적 장애물에 부딪혀 사이버 공격을 빠르게 탐지하고 대응팀에게 필요한 정보를 제공하는 능력을 발휘할 수 없었다.

사이버리스크 관리를 위한 모니터링

반면, 미래의 모니터링 프로그램은 비즈니스에 대한 사이버리스크에 중점을 둔다. 이런 변화는 조직의 더 큰 비즈니스 리스크관리 프로그

사이버보안 융합 센터

리스크 중심의 사이버리스크 관리체제를 갖춘 선도적 기업들은 '융합 센터'를 모델로 삼는다. 융합 센터는 미국 정부가 2001년 9월 11일의 공격 이후 설립한 기관으로, 위협 평가와 대응을 위한 정부기관들 간의 협조를 장려하기 위한 장치다. 융합 센터에서는 다양한 분야의 전문가들이 총체적으로 협조해 갈수록 정교해지고 쉼 없이 변화하는 적대 집단에 적응하는 데 초점을 맞춘다.

이 팀에는 리스크 관리, 내부 감사, 사기 또는 자금세탁 대응, 법률 고문 등 분야의 전문가들이 모여 있다. 기술적 측면에서는 애플리케이션 개발, 시스템과 네트워킹 엔지니어, 사이버리스크 관리, 우선 위협 분석가 등이 포함되어 있다. 직속 상관 또는 지역 리더에게 보고하는 비즈니스 정보 보안 담당자들이 팀을 이끈다. 이런 다양한 구성원들을 가진 팀은 비즈니스 리스크와 사이버리스크에 대한 다채로운 관점을 제시할 수 있을 뿐 아니라 내외부 출처에서 생성된 다양한 데이터, 즉 위협 관련 데이터, 비즈니스 데이터, IT 데이터를 전부 '융합'할 수 있다.

지금처럼 하나의 전문가 그룹이 업무를 다른 그룹으로 넘기기 보다는 통합된 팀이, 특히 그 구성원들이 함께 상주하면, 다양한 비즈니스 영역 전반에서 발생하는 사건들에 대한 지식을 쉽게 공유할 수 있다. 이를 통해 사건 발생 시 더 빠르고 더 효과적인 진단 및 교정이 가능하다.

아마도 가장 중요한 점은 융합 센터가 비즈니스와 사이버리스크 전문가들 간의 이해를 키우는 지속적인 업무 환경을 제공한 점일 것이다. 참가자들은 지속적으로 위협 환경에 대한 이해를 새롭게 할 수 있고 중요한 사이버리스크에 대해 공유된 관점을 개발할 수 있다. 비기술 인력은 기술적 용어나 문제에 익숙해진다. 기술분야 리더들은 비즈니스 프로세스를 더 세밀히 이해할 수 있게 되어 효과적인 모니터링 절차를 정의할 수 있다. 외부의 위협과 비즈니스 자체가 모두 지속적으로 변하기 때문에 융합 센터와 같은 구조야 말로 탐지 역량을 사전에 세밀히 조정할 수 있는 조직 능력의 구심점이다.

램의 일부로 사이버리스크의 기조와 우선순위를 설정하고자 하는 임원 및 이사회의 관여도가 커졌기 때문이다.[9] 이런 변화를 달성하기 위해서는 네 가지 기능 영역에서의 변화가 필요하다.

- **조율.** 최우선 사이버리스크에 대한 전 조직의 수평적 수직적 연계
- **데이터.** 기술적 사건의 탐지보다는 비즈니스 사건의 탐지를 지원할 데이터
- **애널리틱스.** 지표 중심의 접근방식에서 패턴 탐지 접근방식으로의 변환을 위한 애널리틱스
- **인재.** 대응적 행동 모델에서 사전적 행동 모델로의 진화를 가능하게 하는 인재와 인재상

이 네 가지 기능 영역을 더 자세히 살펴보기 전에 차량 렌탈 업체 드라이브나이스가 해킹을 당하기 전에 비즈니스 중심의 사이버리스크 모니터링 프로그램을 갖췄다면 어떻게 대처했을지 살펴보자.(다음 페이지 참조.)

비즈니스 중심의 사이버리스크 모니터링 프로그램을 갖춘 드라이브나이스

이 분야의 여느 회사들과 마찬가지로 드라이브나이스는 첨단 사이버 공격의 대상이다. 앞의 예에서 보듯, 인적 과실로 인해 회사의 업무용 컴퓨터가 회사를 목표로 한 새로운 변종 멀웨어에 감염되었다. 이 멀웨어는 상당히 정교했고, 다양한 지역의 업무용 컴퓨터들을 감염시키기에 충분한 시간 동안 탐지 시스템을 피할 수 있었다.

어느 날, 드라이브나이스의 모니터링 센터로 수많은 보안 관련 경보가 줄줄이 흘러 들어오는 상황에서, 중앙 결제 시스템에 관련된 경고 하나가 높은 우선순위로 발령되었다. 시스템은 자동으로 레벨2 보안 분석가에게 조사 임무를 배정한다. 분석가는 새로운 데스크톱 연결이 이뤄지는 중이란 것을 빠르게 알아챈다. 누군가가 프론트 데스크 직원의 (유효한) 신원정보를 이용해 결제 시스템에 접근을 시도해왔던 것으로 보인다. 분석가는 신속하게 새로운 연결과 관련된 정보의 연관성을 파악하고, 해커들이 동유럽 국가의 인터넷 서비스 제공자(ISP)의 네트워크를 통해 침입 중인 것으로 판단한다. 다른 콘솔에 나타난 위협 정보에 따르면 지금 사용되는 IP 주소는 과거에 범죄 관련 C&C(Command and Control, 공격 지휘통제)활동에 사용된 네트워크와 관련이 있다. 분석가는 빠르게 이 정보를 요약해 사건 요약보고서를 작성하고, 컴퓨터에 설치된 종단 분석도구에서 멀웨어의 코드를 캡쳐해 상세한 포렌직 분석을 위해 제출한다.

물론 이런 분석에 최소 24시간이 걸리기는 하지만, 분석가는 즉각적으로 지역 보안 및 IT 팀에 잠재적인 문제를 알리고, 결제 팀에도 비정상적인 활동을 주시할 것을 경고한다. 드라이브나이스의 모니터링 시스템 내의 워크플로우 기능이 멀웨어의 핵심 특성(지표)을 사이버 방어 팀 및 지역 IT 팀의 툴 전체에 입력한다. 이는 자동적으로 드라이브나이스의 컴퓨터가 멀웨어의 C&C 네트워크에 연결되지 않도록 차단하고, 발견되는 멀웨어 코드를 모두 자동으로 제거하며, 다른 시스템으로의 감염을 막는다.

이런 방법으로 회사의 컴퓨터 네트워크에서 멀웨어를 대부분 제거하고, 지급결제 시스템으로의 침입을 차단하며, 시스템 관리자들은 유사한 감염을 막기 위해 노트북과 데스크톱 시스템의 보안 취약점을 패치한다. 선임 분석가는 CISO의 지원을 받아 몇 주전 유사한 공격을 겪은 다른 회사의 분석가에게서 받은 정보를 비교해, 이번 공격이 같은 멀웨어의 변종인지를 판단한다. 분석가들은 이런 멀웨어가 종종 여러 가지 기능을 수행한다는 것을 알게 되어, 2단계 공격에 대비해야 한다는 것을 깨닫는다.

36시간 이내에 보안 팀은 멀웨어의 속성을 완전히 파악한다. CISO는 즉각 지역 보안 팀과 결제 팀 및 사기 대응팀의 대표들과의 회의를 소집해 발생한 사건을 알리고, 질문에 답하며, 멀웨어가 더 확산되면 겪을 수도 있는 상황에 대해 미리 주의를 준다.

일부 지역 지점의 시스템이 IT 운영 기준을 따르지 않아, 소수의 데스크톱이 감염된 상태로 남아있었다. 이 감염의 결과 멀웨어가 이번에는 나이스리워즈 고객 보상 프로그램을 대상으로 2단계 공격을 시작할 것이다. 중앙 관제 센터에서는 또 다른 높은 우선순위의 보안 경고가 발령된다. 이는 행동 분석 시스템에서 생성한 것으로, 의심스러운 활동과 관련된 것으로 알려진 호주의 네트워크에서 나이스리워즈의 데이터베이스 서버에 접근하고 있음을 경고한 것이다.

몇 분 지나지 않아 업무를 배정받은 분석가는 직접적인 데이터베이스 공격이 진행중인 것을 확인할 수 있었다. 고객 보상 팀에서 전달받은 데이터를 검토한 분석가는 고객들의 보상 포인트 잔액이 고객의 주장과 불일치 하는 경우가 상당 수 발생하고 있다는 것을 파악했다. 이들 계정에서 포인트를 현금화하려는 시도가 짧은 간격으로 반복적으로 일어나고 있

었다. 이런 정보와 멀웨어 분석 결과를 바탕으로 관제팀은 신속하게 호주 프랜차이즈의 IT 팀과 협조해 공격을 막는 작업에 착수한다(기존 친분 관계를 이용해 이를 사법당국에 고지할 수도 있다). 고객 보상팀은 거래가 완료되기 전의 과거 상태로 모든 나이스리워즈 계정을 복구해 놓는다. 재빠른 탐지와 방어작업 결과, 해커들은 방어가 허술한 다른 기업을 목표로 이동한다.

차이를 결정하는 요소

이전의 시나리오와 비교하면, 드라이브나이스는 사이버리스크 모니터링 프로그램에 상당수의 변화를 주었고, 덕분에 이번 해킹 공격의 영향을 크게 제한할 수 있었다.

첫째, 기술팀과 비기술팀이 정기적으로 회의를 갖고 드라이브나이스의 수익흐름, 이익률, 평판을 가장 위협할 수 있는 위험 요소들의 부상을 파악한다. 그 결과 보안 엔지니어들이 모니터링 기술의 설정을 변경해 나이스리워즈의 오용과 부정을 알리는 특정 사건과 패턴을 찾을 수 있었다. 이런 탐지 과정을 위해서는 고객 보상팀, 사기 대응팀, 인사팀에서 받은 비즈니스 데이터의 통합이 필요하다. 이를 위해 정기적인 데이터 전송을 자동화하기 위한 소규모 프로젝트가 진행되었다.

이런 협업의 또 다른 결과로, 드라이브나이스의 클라우드 기반 자산에 대한 모니터링 프로그램의 통합이 결정됐다. 이 과정은 기술적 통합 노력뿐 아니라 서비스 제공자들과의 협상을 위한 비즈니스 측면에서의 노력도 필요했다. 이후 해킹 공격이 일어났을 때, 보안 팀은 의심스러운 활동을 탐지하는데 필수적인 애플리케이션 로그에 대한 가시성을 확보할 수 있었다.

관리자들은 보다 분명하게 정의된 역할과 사기 대응팀과 보상 관련 사이버 운영팀 간, 그리고 다양한 IT 보안 부서 간에도 의사소통 라인을 갖추고 있다. 덕분에 사건이 일

신규 시장 진입, 신규 상품 출시, 효율성 추구, 신규 비즈니스 모델의 수립 등 성장 그 자체를 위해 조직은 리스크를 감수해야 한다. 사이버 위협이 성장과 혁신에 장애가 될 수 있다는 점에 대한 인식과 비즈니스가 언제 실제 위협을 받는가에 대해 가시성을 갖추는 일은 전략적 이익 보호에 필수적이다. 이는 새로운 사이버리스크 모니터링 기능의 핵심 사명이다.

어났을 때, 더 빨리 대화하고 조치할 수 있었다. 지역 팀이 여전히 존재하긴 하지만, 사건 데이터는 중앙 집중화되어 있고, 팀들은 훨씬 더 조직화된 방식으로 운영되며, 중앙 관제팀이 사이버 보안 탐지에 있어 명료한 하향식(Top-down) 권한을 갖고 있다.

비즈니스 리더들은 사이버리스크 활동을 지원해야 한다는 경각심을 갖게 되어, 이제는 일상적으로 애플리케이션과 기술 인프라 변경 전에 사이버리스크 담당자들의 조언을 구한다. 리더들이 관리하는 기술팀은 정기적으로 중앙 모니터링팀에 IT 자산 변경사항 정보를 제공하는 프로그램을 실행하고 있다.

임원들과 비즈니스 리스크 담당 리더들은 이제 드라이브나이스의 모니터링 프로그램에 확신을 갖게 되었고, IT 리더들은 새로운 기술 투자에 관한 지원을 이끌어내기 수월해졌다. 최종 사용자 행동 애널리틱스 프로그램의 실행은 분석가들에게 개선된 패턴 탐지 역량을 부여해, 이전에는 알려지지 않았던 사이버 공격 전술을 파악할 수 있게 되었다.

네 가지 핵심 혁신 영역

두 **번째** 시나리오에서 드라이브나이스의 성공 사례는 단순히 기술 개선 혹은 경영진의 자각에만 기인했다고 볼 수 없다. 이런 성공을 위해서는 어떤 기업이든 네 가지 핵심 영역의 변환을 통한 진화를 이뤄야 한다. 네 가지 핵심 혁신 영역은 드라이브나이스가 멀웨어 공격을 막고 위협을 피할 수 있도록 도움을 줬다.

핵심 비즈니스 리스크를 중심으로 조율

비즈니스 리더들과 이들이 관리하는 기술팀은 사이버리스크팀과 적극적으로 협력해 사업이 직면한 핵심 사이버 리스크에 대한 공유된 관점을 개발하고, 핵심 리스크 관리지표를 정의한다. 핵심 리스크 관리지표는 비즈니스의 필수적 운영 및 프로세스에 피해를 입힐 수 있는 사이버 전장의 위협들을 가리켜 준다. 이 지속적인 과정을 위해, 일부 조직은 구조조정이 필요할 수 있고, 새로운 기능, 부서, 또는 위원회 설립이 필요할 수도 있다(삽입글 '사이버 보안 융합 센터' 참조). 비즈니스 관련 애플리케이션과 프로세스의 운영 절차를 세밀하게 이해한 엔지니어들은 적절한 대상에 대한 모니터링 솔루션을 만들 수 있고, 사이버리스크의 상황에 대해 경영진과 비즈니스 리더들에게 보고하는 능력 또한 개선할 수 있다.

리더들은 기업 전체에 의사소통 채널과 역할을 명확히 지정함으로써 이런 변화를 이끌 수 있고, 사이버리스크 분석가들은 사이버 공격의 탐지, 모니터링, 분석, 대응을 지원받기 위해 내부 또는 외부의 누구에게 도움을 청해야 하는지 알게 된다. 이와 유사하게 사이버 모니터링 담당부

서는 모든 이해관계자들에게 의미 있는 정기 보고서를 작성해 사이버리스크 관련 개선내용과 취약 영역을 요약 보고하며, 업무 조율의 유지를 도울 수 있다.

적절한 데이터

위에서 논한 것처럼, 관제팀에는 데이터가 물밀 듯 들어온다. 하지만 모든 데이터가 중요한 문제를 탐지하는 데 적절한 데이터는 아니다. 사이버리스크 탐지에 비즈니스 중심의 접근법을 취함으로써 엔지니어들은 그들이 포착하는 데이터의 처리에 있어 좀 더 목표지향적이 될 수 있고, 분석가들은 단순한 기술적 사건 보다는 사이버 비즈니스 사건을 탐지하는 데 필요한 데이터를 갖출 수 있다. 비인가자가 특정 시스템에 접근하는 등의 기술적 사건은 사이버 분석가가 해당 시스템이 핵심 비즈니스 프로세스의 일부라는 것을 인지하면 비즈니스 사건이 되며, 이를 잠재적 위협으로 연결할 수 있는 맥락을 가지게 된다.

핵심은 사이버 관제팀에게 IT와 비즈니스, 공격 사이의 연관성을 파악하는 데 필요한 사업부내 다양한 부서에 있는 적시성 및 관련성을 가진 데이터에 대한 접근 권한을 부여하는 것이다. 그 방식은 기업마다 다르겠지만, 여기에는 모든 조직에 있어 기술적 장비 데이터 이상의 데이터에 대한 접근 권한이 포함될 것이다. 일반적으로 이런 데이터에는 현재 직원, 협력사 그리고 기업 자원에 접근 가능한 계약업체들의 명단이 포함되기도 한다. 또한 광범위한 비즈니스 거래 데이터, 재고 데이터, 고객 서비스 기록 등도 포함될 수 있다.

더 나은 정보수집과 자동화를 위한 애널리틱스

의미 있는 위협 활동을 탐지하기 위한 '최종 단계'의 노력은 항상 인적 요소가 중요하다. 하지만 자동화된 정보 시스템 없이는 방대하고 복잡한 환경에 걸친 위협을 인지하기란 사실상 불가능하다. 대부분의 기업 사이버 정보보안팀은 오늘날 보안 정보, 사고 관리, 또는 기타 도구를 통해 사람이 관심을 기울여야 하는 정보를 걸러 내거나 그 연관성을 찾는데 도움을 받는다. 일부 조직은 현재 가진 것들을 더 효과적으로 이용해 상당한 개선을 이룰 수 있다.

그러나 대부분의 전통적 모니터링 툴은 과거의 위협만을 탐지할 수 있다. 왜냐하면 이미 알려진 위협 '신호'의 데이터베이스에 정보를 대조하는 방식에 의존하기 때문이다. 공격은 매일 달라지고, 탐지를 피할 수 있는 악성코드도 많다. 기업들은 기존 시스템을 패턴 또는 변칙성 중심의 접근법을 지원하는 신기술로 강화할 필요가 있다. 첨단 애널리틱스 기술은 훨씬 더 다양한 형태의 대규모 데이터를 다룰 수 있을 뿐 아니라, 더 중요하게는 조직이 자체적인 위협 정보를 만들 수 있는 유연성을 제공한다. '정상적' 상황이 어떤 형상인지, 즉 일상적 네트워크 트래픽 패턴, 비즈니스 거래의 규모, 개인 네트워크 사용자의 행동 등이 어떤가를 이해함으로써, 사이버리스크 관리팀은 더 빠르고 정확하게 현재 진행중인 공격을 가리키는 이상신호를 탐지할 수 있다. 위협 '지표'가 빠르게 변하고, 해커들 또한 빈번히 접근법을 바꾸므로, '정상적' 패턴과 다른 예외 상황의 탐지에 더 집중하면 철저한 조사를 정당화할 수 있는 데이터를 발견할 확률도 커진다.

인적 요소는 여전히 중요하다

전 세계의CIO와 CISO들은 사이버 보안 분야의 기술 인재 부족 현상을 너무나 잘 알고 있다. 하지만 기업들은 더 숙련된 인력뿐만 아니라 새로운 접근법도 필요하다. 목격한 현상에 대응하는 것 보다는 어떤 일이 일어날 수 있는지를 주 업무로 생각하는 분석가들을 위해 새로운 역할이 정립되어야 한다. 알려진 시스템 취약점의 패치는 여전히 중요하지만, 사이버리스크 팀은 이전에 누구도 탐지 못했던, 또는 쳐다 보지도 않았던 허점을 찾을 수 있어야 한다.

모든 직급의 분석가들과 사이버 엔지니어들은 핵심 비즈니스 프로세스를 면밀히 이해해야 한다. 그래야만 보안 사

건 발생 시 그 비즈니스적 맥락을 이해하고 더 나은 탐지 메커니즘을 설계할 수 있다. '기술 전문가'가 되는 것만으로는 충분치 않다. CISO도 마찬가지다. CISO는 조직 전반의 비즈니스 부서들의 참여를 증진할 수 있는 능력이 있어야 한다.(CISO의 역할 변화에 대해서는 이번 호의 '새로운 정보보안 최고책임자(CISO): 전략적 보안 조직을 이끌기'를 참조.[10]) 역으로 최고 경영진과 관리자들은, 특히 전략적 비즈니스 혁신을 주도하는 데 관여하고 있다면, 내부 또는 외부 전문가들을 상대할 때 사이버리스크에 대해 충분히 알고 있어야 한다. (그림 1 참조)

새로운 모니터링 기능을 위해

신규 시장 진출, 신상품 출시, 효율성 추구, 신규 비즈니스 모델의 수립 등 성장 그 자체를 위해 조직은 리스크를 감수해야 한다. 사이버 위협이 성장과 혁신에 장애가 될 수 있다는 인식과 비즈니스가 언제 실제 위협을 받는가에 대한 가시성을 갖추는 일은 전략적 이익 보호에 필수적이다. 이는 새로운 사이버리스크 모니터링 기능의 핵심 사명이다.

이는 '분해와 대체 (Rip-and-replace)' 프로세스나 획기적인 구조조정 노력이 필요한 것이 아니며, 경영진이 이미 실행한 사이버보안 관련 투자를 철회해야 한다는 압박을 느낄 필요도 없다. 이는 수년까지는 아니더라도 몇 달에 걸쳐 이뤄져야 할 필요가 있는 현존하는 역량의 큰 변환과정이다, 다행히 이는 반복적인 과정으로, 과거의 노력에 기반해 계속 강화될 수 있다(되어야 한다).

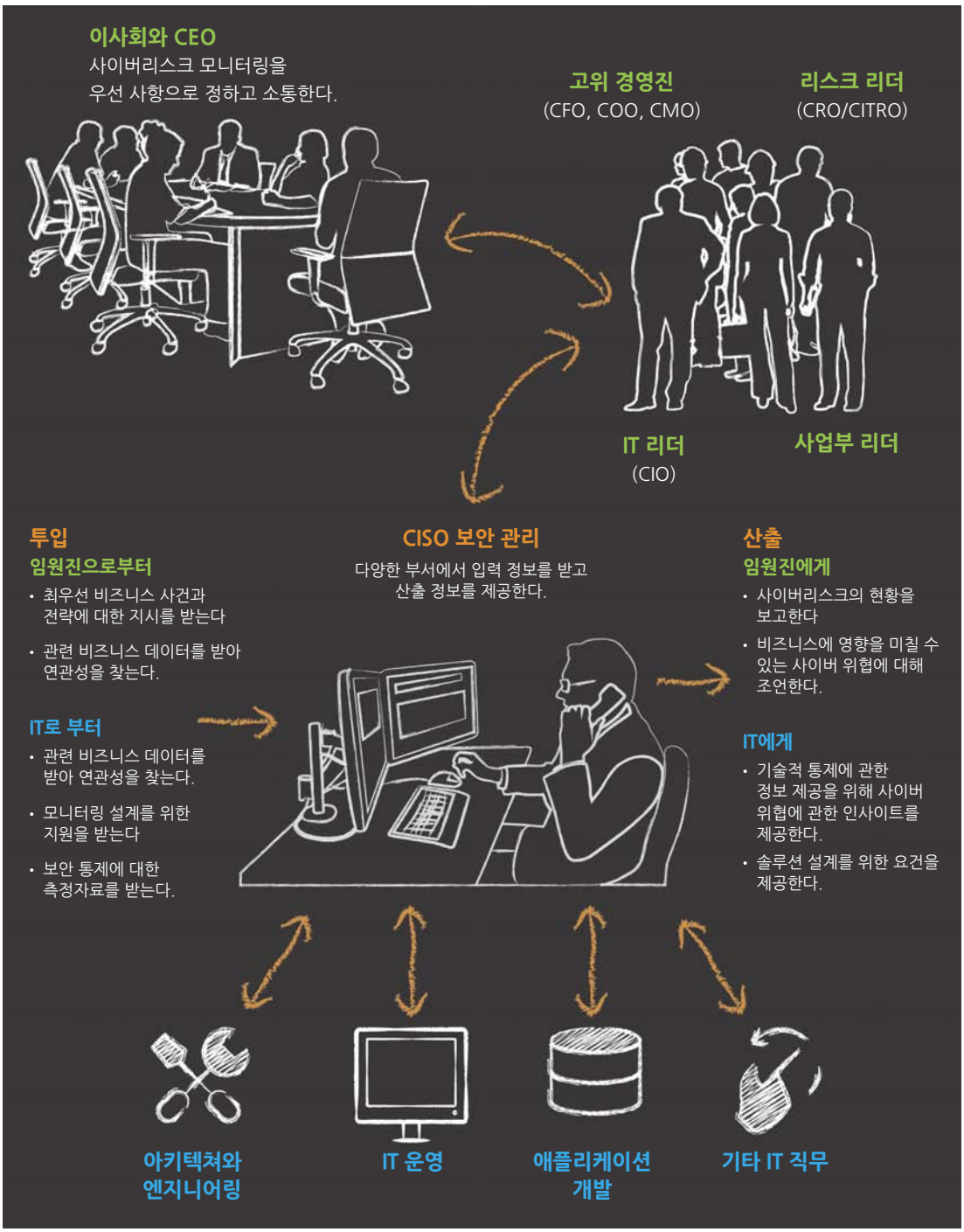
모든 조직은 사업부분이 우려해야만 하는 핵심 사이버리스크 영역에 관해 최고경영진 수준의 지도가 필요하다. 사이버 보안에 경각심을 가진 이사회가 이미 있고, 사이버리스크를 전사적 리스크관리 프레임워크에 통합해 온 조직은 분명한 우위를 가질 수 있을 것이다.

각 사업부와 부서 수준의 리더들은 사이버리스크와 비즈니스리스크간의 통합에 적극적으로 앞장서야 한다. 비즈니스적 측면에서, 조직은 사이버 위협 및 사이버 모니터링과 관련해 상위 수준에서의 개념에 정통하거나 정통하고자 하는 인력이 필요하다. 기술적 측면에서, 책임자인 CIO 또는 CISO가 비즈니스 리스크 관리에 필요한 요건을 설정하는 데 있어 다른 비즈니스 리더들의 참여를 효과적으로 이끌어낼 수 있어야 한다. 이런 요건은 사이버리스크 모니터링 직무의 기조를 정하는 데 필요하다. 일부 조직에서 소수의 리더들은 경영진이 인지하지 못하는 사이에 제대로 된 방향으로 리스크 관리 추진계획을 이끌어가고 있을 수도 있다. 이를 인지하고 추가적인 지원을 제공함으로써 이런 시험적 활동에 속도를 붙여 조직 내 다른 부문에서도 같은 노력을 이끌어낼 수 있다.

마지막으로, 새로운 환경에 적응하기 위해 모니터링 기술의 실질적인 수립 또는 확장을 이끌기에 충분한 엔지니어링 인재, 운영 관리자, 기술 등이 필요하다. 그러나 이 모든 노력이 전적으로 기술적 난관에 관한 것은 아니다. 사람들은 너무나도 자주 만병통치약이 있다는 생각을 하곤 한다. 이는 신기술, 솔루션, 기술 공급자가 오늘날 보안 모니터링상의 모든 허점을 해결할 수 있으리라는 희망 사항에 불과하다. 그보다는 현재 도입되어 있는 툴과 기술을 적절한 업무기술과 비즈니스 협업을 통해 더 효율적으로 이용할 수 있다.

조직이 성숙해서 현재는 유용한 도구와 기술의 경계 및 한계에 일단 직면하게 된다면, 이를 해결할 수 있는 첨단기술에 관한 많은 선택사항이 존재한다. 이들 기술은 풍부한 애널리틱스를 기반으로 하는 '사이버 사냥' 접근법에 적합한 플랫폼을 제공할 수 있다. 사이버 사냥 접근법은 훈련된 분석가들이 공격을 미리 탐색하고 예측까지 할 수 있도록 지원한다. 도구들의 정교함과는 무관하게, 의미있는 결과를 도출하는 일은 기본 원칙에 달려있다. 비즈

그림 1. 사이버리스크 모니터링 프로그램에 관한 전사적 참여



참고: CEO=최고 경영자, CFO=재무 담당 최고책임자, COO=운영 담당 최고책임자, CMO=마케팅 담당 최고책임자, CRO=리스크 담당 최고책임자, CITRO=IT리스크 담당 최고책임자, CIO=정보 담당 최고책임자

그래픽: Deloitte University Press | DUPress.com

조직이 성숙해서 현재는 유용한 도구와 기술의 경계 및 한계에 일단 직면하게 된다면, 이를 해결할 수 있는 첨단기술에 관한 많은 선택사항이 존재한다. 이들 기술은 풍부한 애널리틱스를 기반으로 하는 '사이버 사냥' 접근법에 적합한 플랫폼을 제공할 수 있다. 사이버 사냥 접근법은 훈련된 분석가들이 공격을 미리 탐색하고 예측까지 할 수 있도록 지원한다. 도구들의 정교함 수준과는 무관하게, 의미 있는 결과를 도출하는 일은 기본 원칙에 달려있다. 비즈니스 및 사이버리스크 실무자들은 어떤 비즈니스 리스크를 해결해야 하고, 어떤 리스크 지표가 가장 중요한지 함께 판단을 내린 후에 방법론, 데이터, 기술에 초점을 맞춰야 한다.

니스 및 사이버리스크 실무자들은 어떤 비즈니스 리스크를 해결해야 하고, 어떤 리스크 지표가 가장 중요한지 함께 판단을 내린 후에 방법론, 데이터, 기술에 초점을 맞춰야 한다.

모니터링 역량을 혁신하려는 활동은 '살아있는' 노력이다. 지속적인 거버넌스가 모니터링 프로그램을 계속해서 개선하고 지원하는 협업 문화를 유지하는 데 필요하며, 이를 통해 기술팀의 요청에 적절한 우선순위가 부여되고, 기술팀과 비즈니스팀이 비즈니스 리스크의 환경에 대한 이해를 계속 공유할 수 있게 해야 한다. 오늘날의 빠른 비즈니스 진화 속도를 감안할 때, 일부 위협들이 가장 강력한 보안 통제마저 피할 수 있다는 점은 피할 수 없는 사실이다. 따라서 효과적인 위협 탐지는 비즈니스의 성장을 보호하는 데 필수적이다. 사이버 보안이 매우 어려운 난관으로 보일 수 있지만 희망은 있다. 경영진이 데이터, 애널리틱스, 인재의 활용을 핵심 비즈니스 리스크와 연계하는 데 앞장선다면, 조직은 수동적인 사이버보안 탐지 체제에서 능동적인 사이버리스크 관리 체제로 변화를 시작할 것이다. **DR**

애드넌 암자드(Adnan Amjad)*는 딜로이트 & 투쉬LLP의 파트너로, 취약성 관리, 보안 운영 설계, 관리된 보안 운영, 사이버 공격 관리 애널리틱스 등의 서비스를 제공하는 비질런트(Vigilant) 사업부를 이끌고 있다.*

마크 니콜슨(Mark Nicholson)*은 딜로이트 & 투쉬LLP의 프린시펄이며 비질런트 사업부의 리더로, 금융산업에 주로 서비스를 제공한다.*

앤드류 더글러스(Andrew Douglas)*는 딜로이트 & 투쉬LLP의 디렉터이며 사이버리스크 서비스 그룹의 전문가로서 고급 사이버 테스팅을 담당한다.*

크리스토퍼 스티븐슨(Christopher Stevenson)*은 딜로이트 & 투쉬LLP의 디렉터이며 실시간 전자 거래 구축, 시장 데이터, 금융기관과 거래소의 리스크 관리 시스템에 대한 폭넓은 경험을 갖고 있다.*

이 글의 작성을 주도하고, 도움을 준 ***베스 럭(Beth Ruck)****에게 감사하며* ***키스 브로건(Keith Brogan)****,* ***아이작 콘(Isaac Kohn)****,* ***제이크 스코니키(Jake Skoniecki)****에게도 감사의 말을 전한다.*

Endnotes

1. James Carder, "7 significant insights from the CyberEdge cyberthreat defense report," LogRhythm, February 10, 2016, https://logrhythm.com/blog/7-significant-insights-from-the-cyberedge-cyberthreat-defense-report/.
2. Investment in security information and event monitoring tools alone is estimated to have a compound annual growth rate of 7 percent annually. Gartner, "Forecast analysis: Information security, worldwide, 4Q15 update: IT spending by segment in current dollars, worldwide, 2013–2019 (millions of US dollars)," March 22, 2016.
3. Damballa reports that, daily, "the devices within its average customer's network generate an aggregate average of more than 10,000 events that may potentially be associated with malware behavior." Damballa, *State of Infections Report Q1 2014*, www.damballa.com/damballa-q1-2014-report-shows-average-enterprise-generates-10000-security-events-daily/.
4. In the United States, more than 209,000 jobs in cybersecurity are unfilled, and postings are up by 74 percent. These numbers are expected to grow in the following years. Ariha Setalvad, "Demand to fill cybersecurity jobs booming," Peninsula Press, March 31, 2015, http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/.
5. Cisco, *Cisco Visual Networking Index: Forecast and methodology, 2014–2019 white paper,* May 26, 2015, www.cisco.com/c/en/us/solutions/collateral/service-provider/ip-ngn-ip-next-generation-network/white_paper_c11-481360.html.
6. With the growth of underground marketplaces, malware authors have a financial incentive to find new and up-to-date exploits. See Bromium Labs, *Endpoint Exploitation Trends 2015*, 2016, www.bromium.com/sites/default/files/rpt-bromium-threat-report-2015-us-en.pdf.
7. Neither of these scenarios intentionally represents the circumstances or events of any particular company.
8. A December 2013 study found that no anti-virus scanners had 100 percent detection rates, although the highest was 99.9 percent effective. Many anti-virus programs produce false positives, adding to unnecessary noise. See AV-Comparatives, *Whole product dynamic "real-world" protection test*, December 10, 2013, www.av-comparatives.org/wp-content uploads/2013/12/avc_prot_2013b_en.pdf.
9. For more information on how boards and other leaders can drive cybersecurity changes within their organizations, see Taryn Aguas, Khalid Kark, and Monique François, "The new CISO: Leading the strategic security organization," *Deloitte Review* 19, July 2016, http://dupress.com/articles/ciso-next-generation-strategic-security-organization
10. Ibid.